DRAFT

Department of Defense & Federal

Biometric System Protection Profile for Medium Robustness Environments

Version 0.02

March 3, 2002

D R A F T

Forward

This Protection Profile (PP) was developed to identify and set forth the security requirements for the US Government's biometric system in environments requiring Medium robustness, based on Version 2.1 of the "Common Criteria", International Standard 15408. The Common Criteria can be found at http://csrc.nist.gov/cc.

Comments on this PP should be forwarded to Anne Kong at anne.kong@hqda.army.mil or Swati Shah at shah@itd.nrl.navy.mil.

Protection Profile Title:

DoD and Federal Biometric System Protection Profile for Medium Robustness Environments.

Criteria Version:

This Protection Profile (PP) was developed using Version 2.1 of the Common Criteria (CC).

Constraints:

Targets of Evaluation (TOE) developed to satisfy this PP shall conform to Common Criteria Parts II and III.

Authors:

This PP was prepared by:
Anne Kong, DoD BMO/STS International, Inc.
Andrea Griffith, DoD BMO/STS International, Inc.
David Rhude, National Security Agency (NSA)
Gary Bacon, NSA/Booz Allen Hamilton
Swati Shah, Naval Research Laboratory (NRL)

Acknowledgement:

The authors would like to acknowledge the significant contributions of the United Kingdom's (UK's) Biometric Working Group who authored the UK's Draft PP for Biometric Devices. Due to its overall relevance, much of their work has been incorporated into this document and is an example of superb international cooperation between member nations.

D R A F T

Table of Contents

List of Figures and Tables

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this PP are largely consistent with those used in the Common Criteria (CC), Version 2.1. Selected presentation choices are discussed here to aid the PP user.

The CC allows several operations to be performed on security requirements; *refinement*, *selection, assignment*, and *iteration* are defined in Paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.

> The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. For example, see FIA_UAU.3 in this PP.
>
> The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.* For an example, see FIA_AFL.1 in this PP.
>
> The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets [assignment_value]. For an example, see FIA_AFL.1 in this PP.
>
> The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier (iteration_number). For example, see FMT_MOF.1(1) in this PP.
>
> The **security target writer** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words "determined by the security target writers". For example, see FMT_MTD.1 in this PP.

As a vehicle for providing a further understanding of and context for security requirements, "Application Notes" have been selectively added to this PP. When they appear in the text, these follow either a component or set of components. They provide a discussion of the relationship between security requirements so that the PP user can see why a component or group of components were chosen and what effect it is expected to have a s a group of related functions. As an example, see the Application Notes for FMT_MTD.1.1(2).

Terminology

In the Common Criteria, many terms are defined in Section 2.3. of Part 1. The following are a subset of those definitions and are listed here to aid the reader of the PP. Relevant definitions are included here for convenience.

Common Criteria and PP Terminology

Authentication Data – Information used to confirm the claimed identity of a user.

Authorized External IT Entity – Any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Authorized Administrator – A role which human users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

External IT Entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Human User – Any person who interacts with the TOE.

Identity – A representative (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Level of Robustness – The characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly to support the level of concern assigned to a particular information system. The Global Information Grid (GIG) Information Assurance policy, reference 4 defines three levels of robustness for the DoD: High, Medium, and Basic.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.

Strength of Function (SOF) – a qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms. SOF-basic, SOF-medium, and SOF-high are the three levels of TOE strength of function.

SOF-medium – A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a medium attack potential as defined in Section 1.2.

Target of Evaluation (TOE) – An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

User – Any entity (human user or external IT entity) outside of the TOE that interacts with the TOE.

Biometric Terminology

Attacker - An attacker is any individual who is attempting to subvert the operation of the biometric system. The intention may be either to subsequently gain illegal entry to the portal or to deny entry to legitimate users.

Attempt – The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

Authentication/Authenticate, Biometric – The one-to-one process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with Biometric "Identification".

Behavioral Biometric – A biometric, which is characterized by a behavioral trait that is learned and acquired over time as opposed to a physiological characteristic.

Best Match – The biometric presented is not 100% exactly the same as the reference user template but is the closest match.

Biometric – A measurable, physical characteristic or personal behavioral trait used to authenticate the claimed identity of an enrollee.

Biometric Data – The extracted information taken from the biometric sample and used either to build a reference template or to compare against a previously created reference template.

Biometric Sample – Data representing a biometric characteristic of an end-user as captured by a biometric system.

Biometric System – An automated system capable of capturing a biometric sample from an end user, extracting biometric data from that sample, comparing the biometric data with that contained in one or more reference templates, deciding how well they match, and indicating whether or not an authentication of identity has been achieved.

Capture – The method of taking a biometric sample from the end user.

Comparison – The process of comparing biometric data with a previously stored reference template or templates.

Enrollee – A person who has a biometric reference template on file.

Enrollment – The process of collecting biometric samples from a user and the subsequent preparation, encryption, and storage of biometric reference templates representing that person's identity.

Exact Match – The biometric presented is 100% exactly the same as the reference user template.

False Acceptance – When a biometric system incorrectly identifies an individual or incorrectly authenticates an impostor against a claimed identity.

False Acceptance Rate (FAR) – The probability that a biometric system will incorrectly identify an individual or will fail to reject an imposter. It is stated as follows:

FAR = NFA/NIIA
FAR=NFA/NIVA

Where **FAR** is the false acceptance rate
Where **NFA** is the number of false acceptances
Where **NIIA** is the number of imposter identification attempts
Where **NIVA** is the number of imposter verification attempts

False Rejection – When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False Rejection Rate (FRR) – The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. It is stated as follows:

FRR=NFR/NEIA or **FRR=NFR/NEVA**

Where **FRR** is the false rejection rate
Where **NFR** is the number of false rejections
Where **NEIA** is the number of enrollee identification attempts
Where **NEVA** is the number of enrollee verification attempts

Goat – A biometric end user whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.

Hill Climbing Attack – A type of malicious attack directed towards the comparison process whereby an unauthorized user incrementally increases the proposed matching data and presents this data directly into the comparison function until a successful matching score is provided by the biometric algorithm.

Identification/Identify, Biometric – The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than authenticate a claimed identity. Contrast with "Authentication".

Imposter – A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is a legitimate enrollee.

Match Score – A numeric value or set of values derived from the comparison by the biometric system of a biometric sample with a template.

Piggy-back Attack – A type of malicious attack whereby an unauthorized user gains access to the protected assets through simultaneous entry with an enrollee. This attack may be characterized by physical force or logical entry beyond the portal.

Portal – The logical or physical point beyond which the protected assets reside. For example, a physical portal may be the locking mechanism on a door. A logical portal may be an authentication measure taken prior to gaining access to a computer.

Physical/Physiological Biometric – A biometric, which is characterized by a physical characteristic rather than a behavioral trait.

Replay attack – An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of an imposter attack.

Secure State – A condition of normalcy, which occurs when all functions operate securely, as designed.

Template – Data that represents the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Threshold – The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold may be adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Verification, Biometric – The biometric process of either identifying or authenticating a user.

Zero Effort Forgery – An arbitrary attack on a specific enrollee identity in which the imposter masquerades as the claimed enrollee using his or her own biometric sample.

Document Organization

Section 1 is the introductory material for the PP.

Section 2 provides a general definition for biometric systems.

Section 3 is a description of the biometric system Target of Evaluation (TOE) and its expected environment. This section also discusses the assumptions that must be true about aspects such as physical, personnel, and connectivity conditions. It further defines the set of threats and policies that are to be addressed by either the technical countermeasures implemented in the biometric system or through the environmental controls.

Section 4 defines the security objectives for both the biometric system TOE and the environment in which the biometric system resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the biometric system.

Section 6 provides a rationale to explicitly demonstrate that the security objectives satisfy the identified threats and policies. The section then explains how the set of requirements are complete relative to the objectives; that each security objective is addressed by one or more relevant component requirement(s).

References

Acronyms

Appendix A delineates the U.S. biometric performance standards defined by the Department of Defense (DoD) Biometrics Management Office (BMO).

Appendix B lists the cryptographic algorithms approved for use with biometric systems.

D R A F T

Department of Defense and Federal Biometric System Protection Profile

for Medium Robustness Environments

1. PROTECTION PROFILE (PP) INTRODUCTION

1.1. PP Identification

Title: DoD and Federal Biometric System Protection Profile for Medium Robustness Environments

Authors: Anne Kong, DoD BMO/STS International, Inc.
Andrea Griffith, DoD BMO/STS International, Inc.
David Rhude, National Security Agency (NSA)
Gary Bacon, NSA/Booz Allen Hamilton
Swati Shah, Naval Research Laboratory (NRL)

CC Version: CC Version 2.1

PP Version: Version 3, dated March 2002

Registration: N/A

Keywords: biometrics, information assurance, portal security, protection profile, identification, authentication, verification

1.2. PP Overview

This Protection Profile (PP) specifies the minimum functional and assurance security requirements for biometric systems employed by the U.S. Department of Defense (DoD) and Federal Agencies to provide identification and authentication allowing access control to physical facilities as well as to information systems in medium robustness environments. The information assets protected by the biometric systems specified in this PP are classified as: Unclassified For Official Use Only (FOUO) in DoD systems or Sensitive But Unclassified (SBU) in Federal systems.

The requirements section of this PP specifies a need to encrypt biometric templates. Specifically, all biometric templates must be encrypted while in transit and storage. For the medium robustness PP, the encryption must meet at a minimum the FIPS 140-2 level 3 security requirements.

This PP covers Biometric Application Programming Interface (BioAPI) compliant biometric products of all biometric technologies. Biometric systems are enabling

technologies designed to augment existing security measures by positively identifying and authenticating individuals based on measurable physical features or behaviors.

1.3. Related Protection Profiles

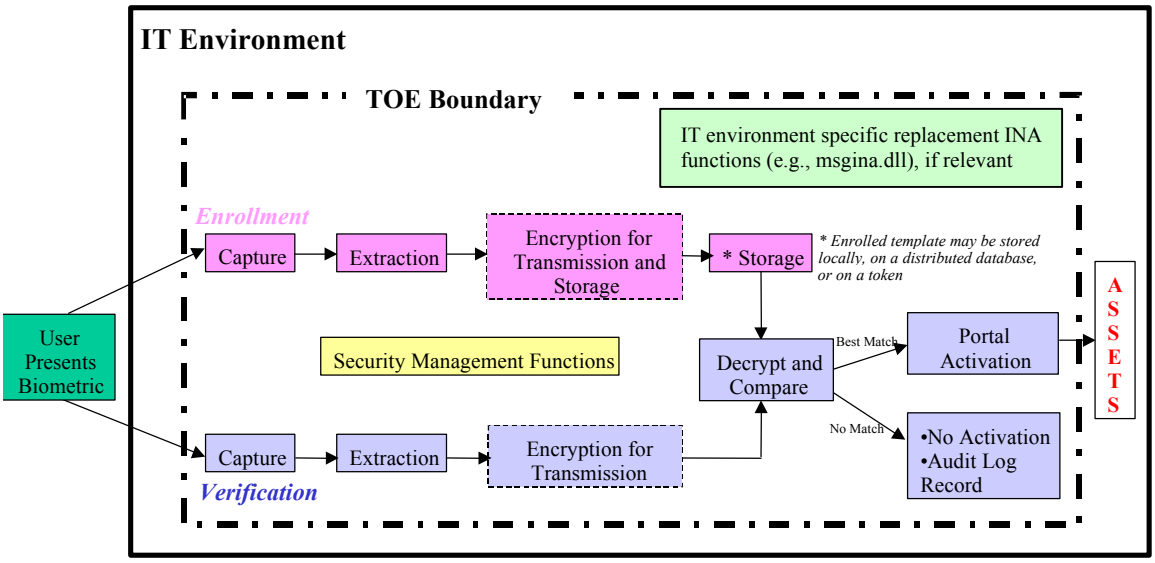
All U. S. Government Protection Profiles (PPs) listed below as related PPs can be found at http://www.iatf.net:

- DoD Public Key Infrastructure (PKI) and Key Management Infrastructure Token Protection Profile (Medium Robustness), Version 3.0 (24 January 2002).
- Protection Profile for Single-Level Operating Systems in Environments of Medium Robustness, Version 1.01 (26 October 2000).
- United Kingdom Biometric Devices Protection Profile (Draft) – *available at http://www.cesg.gov.uk/technology/biometrics*.

2. TARGET OF EVALUATION (TOE) DESCRIPTION

The TOE biometric system performs two processes as shown on Figure 2-1: Enrollment and Verification. The TOE boundary encompasses the functions needed for these two processes, the biometric system's security management functions [e.g., setting security thresholds (if applicable), auditing, enrollment management, allowing manual entry] and management of any IT environment replacement Identification and Authentication (INA) functions [e.g., operating system Graphical INA (GINA) dynamic link libraries (dll)]. The following paragraphs describe the required functions for the TOE. All the functions are required but are NOT restricted to be performed in the sequence shown.

Figure 2-1: Biometric System High Level Functional Architecture



2.1 Enrollment Process

The Enrollment process involves the following required functions:

- Capture – acquiring the "live" individual's physical or behavioral characteristic known as a biometric sample
- Extraction – converting a captured biometric sample into a biometric template of sufficient quality so that it can serve as a reference template for the user being enrolled
- Encryption – encrypting the reference biometric template during transmission between functional components and during storage to protect it against disclosure and modification
- Storage – storing the reference biometric template for later verification. Templates may be stored locally, on a distributed database, or as a user-held template on a token. The TOE will be required to maintain confidentiality, authenticity (e.g., non-repudiation -- proof

of origin) and integrity of the biometric template, regardless of where it is stored.

The users' enrollment process may be supervised and performed only by an administrator. Or, it may be un-supervised, if the user is permitted to self-enroll by the administrator.

2.2 Verification Process

The Verification process involves identification (one-to-many comparison) or authentication (one-to-one comparison). The following functions are required for the authentication process:

- Capture – acquiring the individual's "live" (real time sample) physical or behavioral characteristic known as a biometric sample
- Extraction – converting a captured biometric sample so that it can be used for comparison
- Encryption – encrypting the biometric data for transmission between functional components to protect it against disclosure and modification
- Decrypt & Compare – matching/comparing the biometric data against stored enrolled templates after decryption and ensuring template authenticity (i.e., proof of origin). For identification systems, the biometric sample is compared against all enrolled templates (i.e., one-to-many comparison). For authentication systems, the biometric sample is of a claimed user identity and thus, is compared against the claimed user's template (i.e., one-to-one comparison).
- Portal Activation – interfacing with the application system to activate the portal (i.e., permit access), based only upon a "best match" comparison. "Exact match" comparison should not activate the portal as it may be a forgery or replay attempt and should be recorded in the audit log.

2.3 Cryptographic Services

Biometric TOEs claiming conformance to this PP are required to implement cryptographic services to provide confidentiality, integrity, and non-repudiation (proof of origin) of stored biometric templates and transmitted biometric data. For biometric systems in medium robustness environments used to protect assets classified as DoD FOUO or Federal SBU, the cryptographic services must be implemented using FIPS 140-2 (level 3) compliant cryptographic modules. In addition to the security requirements specified in this PP for cryptographic support, the FIPS 140-2 publication defines security requirements for cryptographic modules and, thus, applies to biometric systems incorporating cryptography. This is regardless of the cryptographic algorithm used, key length used, or whether the cryptography is implemented in hardware, software, or any combination thereof.

2.4 Fall-Back System

An organizational security policy (P.MANUAL) requires the TOE operating environment to include a manual fall-back system (e.g., physical and/or logical), which would be used in the event of failure of the biometric system or where individual users are unable to use the biometric system. This condition may be because they lack the biometric feature used, or have a disability that prevents successful use, or are temporarily unable to use the system because of injury or medical condition. For the purposes of this PP, such fallback systems are considered to be outside the scope of the TOE and no assumptions are made regarding the use of any fall-back systems.

3. TOE SECURITY ENVIRONMENT

The intent of this PP is to specify both security functional and assurance requirements that apply to commercially available biometric products. This particular section identifies the assumptions, threats, and organizational security policies driving the requirements.

Vendors must ensure that the Security Target (ST) specifies the intended environment of use for the biometric system, since certification will be valid for that environment only.

A TOE compliant with this PP must provide appropriate identification and authentication functions for allowing access control to DoD For Official Use Only (FOUO) or Federal Sensitive But Unclassified (SBU) assets. The protected assets behind the portal may either be information systems or physical structures protecting sensitive operations. DoD information and information systems processing FOUO or SBU data in medium robustness environments are categorized as mission support or administrative. Thus, TOEs compliant with this PP shall protect unclassified assets categorized as mission support or administrative and shall demonstrate an Evaluation Assurance Level (EAL) 4 compliance.

3.1 Assumptions

This section discusses the scope of intended usage of the TOE as well as assumptions about the operating environment (both IT and Non-IT) including physical, personnel, and connectivity issues.

3.1.1 Assumptions about the intended usage of the TOE

A.PORTAL

The biometric system is intended to identify, verify, or authenticate the identity of users for entry via the portal. Once beyond the portal, assets are not protected by the biometric system.

The portal may either be a physical facility or an information system. In the latter case, there may be other logical measures (e.g. access control) to protect the assets once the user has gained entry beyond the portal, but these are not within the scope of the TOE.

3.1.2 Assumptions about the TOE operating environment

A.NO_EVIL

Administrators are assumed to be non-hostile and trusted to perform all their duties in a competent manner.

This assumption is made on the premise that the administrator managing the biometric system is cleared to the level of the protected assets and has complete

access to the assets in the protected environment. It would be significantly easier for a malicious administrator to give away the assets than to perform a hostile action on the biometric system allowing unauthorized access to the assets. Just as system administrators are trusted to manage user accounts on an information system, so should biometric system administrators.

The effect of this assumption is to rule out of scope any threats that may be posed by hostile administrators as a means of properly framing the security problem.

A. ROLES

Both Administrator and User roles are defined in this PP. Depending on the application, two or more individuals may fulfill a single role; alternately, a single individual may fulfill two or more roles. In each case, the characteristics applicable to roles are assumed to be transferred to the individual or individuals filling the roles.

3.1.3 Connectivity assumptions

A.USERTMPL

It is assumed that, if users supply their own biometric template, such as can be found on a token, appropriate security measures will be taken by the responsible approving authorities to protect the authenticity and integrity of the template during its transmission and storage to the card.

3.2. Threats

PP compliant TOEs address the threats listed here. The primary assets requiring protection by the biometric system are not stored in the TOE itself. Rather, the assets comprise such things as information, equipment, people, that may be accessed through entry to the portal. While the threat agent and attack vary for different threats, the motivation is generally the same – to gain illegal entry to the portal controlled by the biometric system, and in turn the assets contained there in or to deny entry to legitimate users.

Note that in some threats, secondary assets may be identified, which if compromised, could leave the primary assets vulnerable to attack. Since the most significant secondary assets are the actual biometric templates, every effort must be made to assure their integrity, authenticity, and confidentiality. In contrast, the security of the primary assets cannot (given the nature of biometric characteristics) rely on the biometric template being kept confidential. In most cases, an imposter's opportunities for attack can be constrained by controlling access to stored templates.

The threat agents may either be authorized or unauthorized users attempting entry beyond the portal through hostile means. Note, however, that it is assumed (A.NO_EVIL) that administrators are not hostile, and hence, such individuals are considered to be threat agents only to the extent that vulnerabilities could arise in administration errors.

3.2.1 Impersonation Threats

One of threats to biometric systems is clearly impersonation. Impersonation occurs when an impostor, masquerading as an enrolled user, attempts to gain unauthorized access to the assets protected by the biometric system. There are a number of forms that the impersonation may take and these are listed as separate threats in this section. There are a number of broad categories of impersonation threats as follows:

- An imposter attempts to defeat the biometric authentication or identification either by a zero-effort forgery attempt (T.CASUAL), through mimicry (T.MIMIC), or by use of an artifact (T.ARTIFACT).

- The attack by the imposter is directed at some known or suspected weakness (T.WEAKID, T.EVILTWIN, T.RESIDUAL, T.POORIMG).

- The attack by the impostor attempts to subvert the identification or verification process by undermining the integrity of biometric templates (T.FAKETEMPL).

As can be seen, there is significant inter-dependency between the threats, and some attacks could be considered to be within the scope of more than one threat. The distinction between mimicry and use of an artifact is not necessarily obvious in all cases. What matters, however, is that the attack is considered and addressed, rather than the precise categorization.

T.ARTIFACT

An imposter may use an artificial hand/fingerprint, life-size photograph, or other synthetic means to gain access.

If an imposter can access a biometric sample or template, he/she may be able to produce an artifact with an equivalent biometric template. Biometric systems unable to detect the difference between the "live" (real time) sample and an artifact may be fooled by the use of such an artifact.

Fingerprint and hand geometry systems are known to be vulnerable to artifacts. The set-up costs are often low making the production of artifacts worthwhile for impostors for common use biometric technologies.

The risk is greatly reduced when supervised systems make some check for liveness, however, supervision does not equal a biometric liveness check.

T.CASUAL

An imposter may make a zero-effort attempt to impersonate an authorized user through mere repetition using his own biometric input.

The attacked identity is randomly chosen and the imposter makes no attempt to modify his/her own biometric characteristics to appear closer to the attacked identity. If the system is an identification system, where the imposter does not claim any particular ID, all IDs are attacked in a single attempt. The chance of such an attack being successful is measured by the False Acceptance Rate (FAR) of the system. The level of threat will be dependent on the residual FAR after the thresholds, which control the balance between FAR and FRR (False Rejection Rate), have been set by the administrator. In some systems an administrator cannot set a FAR and FRR rate.

Such an attempt may be successful if:

- The system has a poor FAR either through technical constraints or through incorrectly set threshold values.
- The impostor has, by chance, a sufficiently close biometric similarity to an authorized user to be able to fool the system.
- The impostor is able to make many unchallenged attempts to gain access. Such attempts may be on a single ID or a range of IDs.

A properly adjusted threshold will likely prevent several unchallenged attempts. Note, that in the case of an identification system, the FAR may be affected by both the size of the database and the demographics of the database population.

T.EVILTWIN

An impostor may attack a similar or twinned ID.

In some cases, an impostor may know that his/her biometric characteristics are very similar to those of an enrollee and attack that identity. This includes physical twins but is not confined to this case. The greater the number of enrollees, the more likely it is that the impostor resembles one of them. Some biometric systems cannot distinguish between twins. Where the biometric system may confuse two individuals, an imposter may know which enrollees they best match and, for example, which finger to use.

The risk is not confined to identical twins. For most cases, identical twins do not have the same biometric properties (e.g. fingerprints, DNA). As a result of FAR limitations, there may be pairs of unrelated individuals within relatively small samples, who can be reliably identified as each other. The administrator can find out which pairs of individuals cannot easily be distinguished by the system by performing inter-template comparisons. Such information should be kept confidential. However, an impostor may discover this information from a similar system elsewhere if the indistinguishable individuals are enrolled on both systems. Also, when an administrator leaves, he/she may take away knowledge of similar IDs and, unlike password-based authentication, it is not possible to change the biometric templates if the knowledge of similarities is seen to present a security risk.

T.FAIL_SECURE

An attacker may cause failure of the TOE security functions by exposing the TOE to conditions outside of its normal operating range, causing the TOE to enter a non-secure state.

T.FAKETMPL

If a user presents a token containing his/her biometric template, it may be forged and actually contain the biometric template of an impostor.

This threat largely applies where the user holds the template and there are no measures to ensure the authenticity and integrity of the template. The obvious countermeasure to this threat is to employ an alternative security measure such as third party template signing. This threat, if successful, will undermine the integrity of enrollment templates.

T.MIMIC

An imposter may be able to reproduce the biometric characteristics of the ID under attack by changing his/her voice, forging a signature, or other means of mimicry.

The imposter may be able to capture the biometric feature used by the system (e.g. record voice, photograph face, video signature, etc.) to gain access to the system and assets. The imposter may then practice mimicry of the biometric feature to give an "accepted" biometric sample. Samples can be automatically (systematically or randomly) generated, like password guessing.

Many biometrics are "public" and can be copied from recorded speech or observing a live signature. Moreover, if someone has been enrolled with the same biometric on several systems, the information may be accessed on the least secure system. In practice, there is little that can be done to reduce the risk that an impostor could obtain public information.

In a supervised system, it is considerably more difficult to successfully mimic an enrollee without being detected.

T.DEGRADE

Installing and using the biometric system may degrade the security of the host IT environment (e.g., Operating System).

For instance, replacing the IT environment's existing INA function with a biometric INA function may compromise the authentication process of the IT environment (depending on how biometric INA function is implemented/configured).

T.POORIMG

An imposter may direct an attack against a noisy or null biometric sample.

Biometric systems may be vulnerable to attack if a noisy sample is unintentionally generated during enrollment. An impostor may also be able to gain illegal entry to the portal if the system accepts a null biometric sample at the time of enrollment.

Some fingerprint systems may treat noise in the sample as if it were minutiae points, and a noisy sample may then produce sufficient agreements with the reference template to pass the verification. With such systems, an imposter may be able to greatly increase the chance of acceptance through the generation of a noisy fingerprint sample or through the construction of an artificial fingerprint exploiting this weakness.

Similarly, voice recognition systems may be vulnerable if the system accepts a sample that is too "quiet". If the enrollee pauses too long before starting to speak, the sample may consist almost entirely of noise. Even if the system implements a "too quiet" threshold for sample acceptance, it may still be vulnerable if the background noise exceeds the threshold.

Clearly, the risk depends on the system. With well-developed technologies, the possible pitfalls are known and checks can be designed within the system to avoid these errors.

T.RESIDUAL

Residual biometric data from a previous valid user if not cleared may be sufficient to allow unauthorized access to an imposter.

There could be a potential risk of reusing an authorized user's biometric sample if the captured biometric sample is not cleared from the capture device after the capture/process functions are completed. Likewise, after the compare function, if an authorized user's biometric data is not cleared, it may allow inadvertent access by an imposter.

Some biometric systems may be vulnerable to residual samples. These could be limited to cases where physical contact with the biometric capture device is involved, such as with fingerprint technologies. If an enrolled user leaves a residual fingerprint on a fingerprint capture device, an impostor may be able to gain subsequent access. This vulnerability may be exploited separately or in conjunction with another vulnerability such as the use of an artifact.

T.WEAKID

An imposter may direct an attack against a weak ID. A weak ID can be caused by poor enrollment procedures that lead to bad or noisy biometric samples and templates with wide thresholds (FAR).

An imposter may attack a specific ID, which is assumed to be weaker than others. If an impostor can identify such users, an attack could be directed against the weak IDs.

Such an attempt may succeed if:

- The FAR is much higher for some IDs than for others, either naturally or through enrollee collusion.
- A poor or noisy biometric sample has resulted in the construction of an insecure template. For example, in the case of signature verification technology, the enrollee might provide a set of signatures with much greater variation than normal.
- An impostor can discover which are the weak IDs. This may happen through collusion, or through finding which IDs have the loosest threshold settings in the database. It is also possible that the decision threshold has been relaxed for some, easily identified individuals who would otherwise have problems in using the system.

The risk will largely depend on the specific biometric technology used. It may be mitigated if weak IDs can be identified and eliminated, perhaps, by re-enrolling weak IDs. This may happen at the time of enrollment or later, perhaps by analysis of inter-template comparisons. Relaxing the decision thresholds to allow "goats" to use the system more easily, or to prevent dignitaries from experiencing false rejection will increase risk.

3.2.2 Threats posed by authorized users

T.BADADMIN

A legitimate administrator may unintentionally compromise the security of the biometric system during routine operations and/or maintenance.

An administrator has specific authority over a regular user. An administrator might inadvertently use this authority to erroneously allow/disallow entry beyond the portal. As previously stated, A.NO_EVIL assumes that administrators will not misuse their authority intentionally.

T.BADUSER

Two types of individuals access the biometric system: Administrators and Users. Regular users with no special privileges may attempt to modify their individual parameters or gain other special privileges normally reserved for administrators.

Only administrators have access to functions that allow individual parameters to be modified.

T.FARFRR

An improperly adjusted FAR or FRR may result in an unauthorized individual entering the portal or an authorized individual being denied entry.

The identifying power of a biometric system is defined by its false rejection rate (FRR) and false acceptance rate (FAR). The desired balance between FRR and FAR may be controlled administratively for some systems. The FAR must be sufficiently small so that no two individuals appear to have the same physical or behavioral characteristic, otherwise an unauthorized person may, under certain circumstances, successfully impersonate another individual. As the FAR and FRR have an inverse relationship, they must be adjusted to suit the particular environment in order to keep the biometric system effective.

Incompetence or inadequate training of administrative personnel could easily result in improperly set FAR/FRR parameters. The probability that an attacker could take advantage of this vulnerability is high. Therefore, user accessibility to these parameters must be tightly controlled.

3.2.3 Threats based on exploitation of vulnerabilities or flaws in the TOE

This section describes a collection of threats where the threat agent is attempting to exploit vulnerabilities in the design, implementation, or operation in order to circumvent the TOE's security functions.

T.BYPASS

An impostor may bypass the capture device or the biometric system entirely.

By collusion or otherwise, an impostor may also gain access to the portal together with an authorized user. An impostor may also be substituted for an authorized user after the authorization operation. This could occur with the collusion of an authorized user or inadvertently, due to distraction. Alternatively, an authorized user may be kidnapped and forced to invoke the authorization process or an impostor may force his/her way through the portal. The risk here is likely to be reduced if the system is supervised or if it is physically designed to allow access to only one person per authorization operation.

T.CORRUPT

An attacker may modify system parameters (FRR/FAR), security-relevant data (user security attributes), and/or executables of the biometric system.

Such an attack could compromise the integrity of enrolled biometric samples or the executables resulting in illegal access to the portal.

The risk of this vulnerability being exploited depends on the resources available to the adversaries and how valuable the assets protected by the biometric system are to the adversaries.

T.UNDETECT

An undetected attack against the TOE security functions is:

(a) An unintentional flaw introduced/existent in the biometric capture device or
(b) An undetected attack mounted by an adversary, which eventually succeeds.

Other sources of noise (e.g., scratches in the fingerprint reader or magnetic interference in a microphone) unintentionally introduced/existent in the capture device could eventually result in exploiting a vulnerability in the TOE security functions.

Proper management and monitoring of the biometric system depends on the ability to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized access modification, or destruction.

An undetected attack, leading to exploitation of vulnerabilities in the biometric system, may occur as a result of:

- Inadequate collection of audit data. The audit parameters might be inadequately set or the audit mechanism may not be strong enough for the intended purpose.
- Unauthorized modification or reset of the audit trail-rendering attacker exploits as undetected.
- Failure of an administrator to properly peruse the audit trails and takes appropriate action when necessary.

One of the motivations of attack is a low probability of being caught. The audit trail serves the purpose of catching attacks after-the-fact and may serve as a deterrent.

T.POWER

A power loss results in failure of the biometric system.

If the power fails and the biometric system becomes inoperable, it may be possible for unauthorized individuals to enter the portal either through being able to exploit vulnerabilities in the fallback system or if the biometric system fails in an insecure manner.

T.REPLAY

An unauthorized user may capture a valid user's biometric authentication data as it is being transmitted between portions of the TOE or from where it is stored, and

replay it at a later time to gain illicit access or used to attack an higher robustness system.

If the connection between the functional components of the TOE can be intercepted during the enrollment or verification processes, it may be possible to capture the transmitted data and later replay the data directly to the authentication component (by evading the capture device) to gain unauthorized access. Additionally, if an adversary were to gain access to stored biometric templates, they may be copied and replayed later. This is commonly referred to as "replay attacks".

3.2.4 Threats based on physical attacks.

This section details threats, which are based on deliberate physical attack against the biometric system.

T.NOISE

The biometric system or its connections are flooded with noise data causing improper functioning of the capture device or comparator, causing an individual to be erroneously allowed or denied entry into the portal.

This type of attack could either allow impostors to enter the portal or result in a denial of service to authorized users. The particular form of noise, which would pose a threat, would depend on the biometric. The main types are electromagnetic flooding (i.e. noise at wavelengths from radio frequency through light to gamma rays) and acoustic noise.

Note that the threat only relates to flooding attacks that occur at the time of identification or verification. Noise may also affect the quality of the enrolled template; however such problems are within the scope of threats T.WEAKID and T.POORIMG.

T.TAMPER

An attacker may modify or otherwise alter the software/hardware components, the connections between them, or the connections between the biometric system and the portal; thereby causing an individual to be erroneously allowed or denied entry to the portal.

This threat includes the tampering attacks against the following:

- The hardware components such as the capture device or the comparator;
- The connection between the capture device and the comparator
- The connections between the comparator and the portal, such that the result of verification is not securely relayed, or an access allowed/denied result is submitted to the connection by means of the biometric system.

3.2.5 Threats Regarding Cryptographic Functions

This section details threats that may be applied to the cryptographic functions employed in the biometric system.

T.CRYPT_ATTK

An attacker may defeat security functions through a cryptographic attack against the algorithm, through cryptanalysis on encrypted data, or through a brute-force attack.

There is no protection against inherent flaws in algorithms. However, given any cryptographic algorithm, there is a list of countermeasures that the implementer should follow.

3.3 Organizational Security Policies

P.MANUAL

A manual means for opening the portal must be provided in the event of a biometric system failure or other emergency to accommodate those users who are unable to provide a sample.

P.SECOP

Individuals responsible for administering and maintaining the TOE must ensure the IT environment's security is sustained by executing routine security procedures on the TOE, e.g., reviewing audit trails, maintaining backups of biometric templates, maintaining proper thresholds of the biometric system, performing periodic security tests on the biometric suite.

P.TRAIN

All individuals who access any security-related system must receive training on the proper use of the system as well as security issues and vulnerabilities.

P.USERLIMIT

Imposters must be prevented from gaining access to the portal by making repeated verification attempts using one or more claimed IDs.

Organizational security policy will establish the maximum number of unsuccessful verification attempts permitted by the biometric system. The administrator will be trained to enforce this policy.

4. SECURITY OBJECTIVES

This section describes the security objectives for the TOE and those for the environment. Section 4.1 delineates security objectives for the TOE, which will be addressed by TOE security functional requirements in Section 5.1. Section 4.2 discusses security objectives

for the environment, which will be implemented within the IT domain by non-technical or procedural means.

4.1. Security Objectives for the TOE

O.ADMIN

The TOE will insure that modification of threshold parameters, security-relevant data, configuration items, audit parameters, and the audit trail is limited to those verified as Administrators by the TOE. The TOE shall provide all the administrative functions necessary to support the management of the TOE security and shall include functions to:

1) Tune the performance of the biometric system (i.e. FAR/FRR thresholds) to meet the DoD defined requirements of the biometric as specified in Appendix A;
2) Maintain the enrolled biometric template database, including verifying the template quality, preventing input of null samples, and providing feedback to the administrator during enrollment to support input of good quality templates;
3) Manage auditing functions such as resetting or modifying the audit trail;
4) Restore the biometric system to a secure state in the event of failure, alteration, or interruption;
5) Verify secure operation of the TOE including accessing and modifying the backing up of data.
6) Allow administrator to set the maximum user limit for unsuccessful verification attempts.

Note that in order to achieve this objective, the TOE will need to identify and authenticate administrators of the TOE. This can be accomplished by means of the TOE's biometric authentication mechanism or by using alternative authentication mechanisms provided by the IT environment. Since there are risks associated with both means, the Security Target will identify and justify the choice of authentication for administrators.

O.BYPASS

The TOE shall prevent illicit individuals or errant software from bypassing the TOE security functions.

Encryption and time-stamping of the signal between the capture device and the rest of the system can help to overcome the vulnerability of bypassing methods such as a replay attack. In such cases, the timestamp should be encrypted with proper encryption technique. Physically designing the capture device to allow access to only one person per authorization operation may help to overcome the vulnerability of bypassing through forced entry.

O.CLEAR

The TOE shall ensure no residual or unprotected biometric data remains after operations are completed.

O.CRYPT

The TOE shall perform cryptographic functions with sufficient strength to protect the enrolled templates from disclosure and modification.

Cryptographic operations must be consistent with established cryptographic usage policies and standards for the level of data being protected by the biometric system.

O.NODEGRADE

Installing and using the biometric system shall not degrade the security of the host IT environment (e.g., Operating System); whereby, the biometric system's replacement Identification and Authentication (INA) function should be no less secure than the IT environment's existing INA function.

O.INIT

An initialized TOE must assume the non-authenticated state immediately upon power-up, reset, or after other restart conditions.

O.KEY_ENCRYPT

Keys stored in non-volatile memory on the TOE must be protected from disclosure or modification through encryption of sufficient strength.

O.NOFORGE

The TOE shall provide the means of performing a liveness check and detecting forgery of authentication data and biometric templates.

Exact Match comparisons may imply a forgery attempt of a biometric template; thus, this security objective will ensure exact match comparison is detected and recorded.

O.PHYSICAL

The TOE shall resist physical attacks against those components of the system, which are critical to security. This shall include the following attacks:

a) Malicious modification or replacement of TOE components (e.g., software/hardware components) or connections between them,

b) Surveillance of physical connections, and

c) Electromagnetic or other relevant noise flooding attacks.

O.RECORD

The TOE shall record necessary events to ensure that the information exists to support effective security management and shall ensure that all TOE users can subsequently be held accountable for their security relevant actions.

O.USERLIMIT

The TOE shall prevent an unauthorized user from gaining access to the portal by making repeated attempts using one or more claimed IDs.

4.2. Security objectives for the environment

O.ENROL

Those responsible for the TOE shall ensure the enrollment process is conducted by trained administrators capable of ensuring that the enrollment is of sufficient quality to maintain security, either as a supervised process or through self-enrollment after validating the user's identity.

Supervision serves to reduce the risk of an insecure enrollment, which could facilitate an easy attack on a weak enrollment template. Procedures should be in-place to permit self-enrollment by trained administrators only as required. Good quality enrollments will also allow decision thresholds to be adjusted so as to provide better discrimination between false acceptance and false rejection rates. This objective also identifies the need for appropriate measures to be taken to authenticate the identity claimed by the enrollee; otherwise security will not be maintained.

O.INSTALL

Those responsible for the TOE must insure that the TOE is delivered and installed in a manner, which maintains IT security.

O.SECOP

Those responsible for the TOE shall ensure that the TOE is managed and operated in a manner, which maintains IT security in accordance with the OSP (i.e., P.SECOP). In particular:

a) Audit trails shall be examined regularly to identify unsuccessful impostor attempts.
b) Acceptance thresholds should be checked regularly to ensure that the biometric system is optimally tuned to maintain the required security levels as specified in Appendix A.
c) Backups of the database containing user security attributes shall be protected against unauthorized access.
d) Entry to the portal shall be supervised where necessary.
e) Periodically perform a suite of tests to demonstrate correct security functions (e.g., to detect attempts of modifying/replacing TOE components and electromagnetic / noise flooding attacks).

If audit trails are not checked on a regular basis, impostors may be able to improve their attempts or find an ID for which they are accepted. Procedures for checking the appropriateness of decision thresholds governing false acceptance and false rejection will help reduce the risk of casual impostor attack on weak IDs and help to identify when it is necessary to re-enroll users. For example, checking the matching results of inter-template comparisons for enrolled users will give some indications of the false accept and reject rates can vary considerably according to the user and impostor populations. Supervision of entry to the portal may be required to help prevent bypass attacks.

O.TRAIN

Those responsible for security of the organization shall provide initial and ongoing training for all individuals. This training should include security awareness of vulnerabilities.

Incompetence or inadequate training of administrative personnel could, for example, easily result in improperly set FAR/FRR values.

O.USERLIMIT

The TOE and/or its environment shall prevent an unauthorized user from gaining access to the portal by making repeated attempts using one or more claimed IDs.

This objective is repeated for both the TOE and its environment, in accordance with [CC1, B.2.5.]. If the TOE does not provide this capability, measures must be taken in the environment to ensure this objective is met (e.g. supervised access).

O.USERTMPL

If biometric templates are supplied by the user (e.g. stored on a token) then appropriate measures shall be provided by the responsible approving authorities to protect the integrity and guarantee the authenticity of the template.

This objective is needed to uphold the assumption A.USERTMPL as well as support O.NOFORGE by providing a means by which the biometric system can detect forgery of user-held biometric templates. Note that this objective also covers the need to protect the delivery path from enrollment to the end-user, for example, covering:

- Delivery of the enrollment template (and other relevant user identification information) to the card production facility,
- Maintenance of the integrity of the template and associated user information during card production, and
- Delivery of the card to the end-user.

5. IT SECURITY REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. These requirements consist of functional components from Part 2 and assurance components from Part 3 of the CC. Table 5.1 summarizes the TOE Functional Requirements to meet the stated objectives.

Table 5.1 – Biometric System Functional Requirements

Short Name	*Descriptive Name*	*Dependencies*
Class FIA: Identification and Authentication		
FIA_AFL.1	Multiple Unsuccessful Authentications	FIA_UAU.1
FIA_ATD.1	User Attribute Definition	None
FIA_UAU.2	User Authentication Before Any Action	FIA_UID.1
FIA_UAU.3	Unforgeable Authentication	None
FIA_UAU.7	Protected Authentication Feedback	FIA_UAU.1
FIA_UID.2	User Identification Before Any Action	None
Class FMT: Security Management		
FMT_MOF.1	Management of Security Functions behavior	FMT_SMR.1
FMT_MTD.1	Management of TSF Data	FMT_SMR.1
FMT_MTD.3	Secure TSF Data	ADV_SPM.1, FMT_MTD.1
FMT_REV.1	Revocation	FMT_SMR.1
FMT_SAE.1	Security Attribute Expiration	FMT_SMR.1, FPT_STM.1
FMT_SMR.1	Security Roles	FIA_UID.1
Class FAU: Security Audit		
FAU_GEN.1	Audit Data Generation	FPT_STM.1
FAU_SAR.1	Audit Review	FAU_GEN.1
FAU_SAR.2	Restricted Audit Review	FAU_SAR.1
FAU_STG.2	Guarantee of Audit Data Availability	FAU_GEN.1
Class FPT: Protection of the Trusted Security Function (TSF)		
FPT_AMT.1	Abstract Machine Testing	None
FPT_FLS.1	Fail Secure	ADV_SPM.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	None
FPT_ITT.3	TSF Data Integrity Monitoring	FPT_ITT.1
FPT_PHP.3	Resistance to Physical Attack	None
FPT_RCV.1	Manual Recovery	FPT_TST.1, AGD_ADM.1, ADV_SPM.1

Short Name	*Descriptive Name*	*Dependencies*
FPT_RPL.1	**Replay Detection**	**None**
FPT_RVM.1	**Non-bypassability of the TSP**	**None**
FPT_SEP.1	**Domain Separation**	**None**
FPT_STM.1	**Reliable Time Stamps**	**None**
FPT_TST.1	**TSF Testing**	**FPT_AMT.1**
FPT_RIP.2	**Full Residual Information Protection (Extended FPT Class SFR)**	**None**
Class FCO: Communication		
FCO_NRO.2	**Non-repudiation of origin**	**FIA_UID.1**
Class FCS: Cryptographic Support		
FCS_CKM.1	**Cryptographic key generation**	**FCS_CKM.2**
FCS_CKM.2	**Cryptographic key distribution**	**FCS_CKM.1, .4**
FCS_CKM.3	**Cryptographic key access**	**FCS_CKM.1, .4**
FCS_CKM.4	**Cryptographic key destruction**	**FCS_CKM.1**
FCS_COP.1	**Cryptographic operation**	**FCS_CKM.1, .4**

5.1. TOE Security Functional Requirements

This section identifies Security Functional Requirements (SFR) for the TOE.

All SFRs are drawn from the standard set listed in CC Part 2[CC2]. In certain cases, these need interpretation to deal with particular characteristics of biometric systems. Advice on interpretation is provided in the form of application notes where necessary. In cases where there are no application notes, the normal interpretation appropriate to IT system security functionality may be assumed.

Uncompleted assignment operations on CC Part 2 functional components are indicated using the same notation as in CC Part 2, e.g. "[assignment:…]" indicates an assignment to be completed by the ST author.

Completed assignment or selection operations are indicated by *italicized and underline* text. Note that in some cases, operations have been *partially* completed within this PP. In these cases, the completed parts are indicated by *italicized* text while the aspects requiring completion by the ST author are indicated using the notation for uncompleted operations indicated above. Refinements of CC Part 2, functional components, are indicated by **bold** text.

Iteration of a component is indicated by the use of numbers in parentheses appended to the CC Part 2 component labels, e.g. FMT_MOF.1(2) indicates the second iteration of the FMT_MOF.1 component.

5.1.1. Identification and Authentication

FIA_AFL.1.1

The TSF shall detect when [assignment: *number specified by an administrator]* unsuccessful authentication attempts occur related to [assignment: *biometric authentication attempts specified by an administrator*].

Application Notes:

The administrator shall specify the maximum number of unsuccessful authentication attempts allowed before the TOE takes action. The TOE Security Target (ST) shall explain how the TOE allows the administrator to set the maximum number. The ST should also provide details of how the administrator is permitted to set the actions taken by the TOE, as stated in FIA_AFL.1.2. It is permissible for the TOE to make no check for multiple attempts, if the administrator specifies a maximum number of unsuccessful attempts as 1.

For a verification system, there are a number of different circumstances that may constitute multiple unsuccessful authentication attempts. Firstly, when the same biometric template (as determined by the TOE within its threshold settings) is used to successively attack a single user identification. Secondly, when different biometric templates (as determined by the TOE within its threshold settings) are successively used to attack a single user identification. Thirdly, when the same biometric template (as determined by the TOE within its threshold settings) is successively used to attack different user identifications.

The TOE may detect each or any of these conditions and the number of unsuccessful authentication attempts allowed may be different for each circumstance. Not all TOEs may be able to distinguish or detect all the different circumstances listed. The Security Target shall state the conditions detected by the TOE in the second assignment. If the number of unsuccessful authentication attempts allowed varies according to each circumstance detected, it will be necessary to iterate FIA_AFL.1 in the Security Target for each such event.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *block any further authentication attempts related to that user until a defined time period has elapsed, as specified by the administrator, and perform any additional measures as specified by the administrator]*.

Application Notes:

This security functional requirement needs to be interpreted in the light of the circumstances, which apply to FIA_AFL.1.1 previously. If the TOE does not detect multiple unsuccessful authentication attempts, then completing the first

assignment with "until the next authentication attempt" should indicate this. This effectively reduces the SFR to a null requirement on the TOE. As with FIA_AFL.1.1, this should be clearly explained in the Security Target.

If the TOE is an identification system, the administrator should complete the assignments so as to reduce the SFR to a null requirement on the TOE, as described above.

For a verification system, the various circumstances delineated previously need further clarification, possibly by iteration of FIA.AFL.1.2. In circumstances where a single use identification is subject to repeated unsuccessful authentication attempts (using the same or different biometric templates), further attempts to authenticate against that user shall be blocked. The Security Target shall state the behavior of the TOE under all relevant circumstances.

The time period referred to in the security functional requirement will need clarification in the Security Target if the TOE implements a more complex time-out scheme for the blocking of unsuccessful authentication attempts.

The TOE may take additional measures when repeated unsuccessful authentication attempts occur. These should be stated in the Security Target by completing the second assignment. If no additional measures are taken, an assignment of "none" should be indicated by deleting the second assignment and the preceding "and".

Under all circumstances, auditing is to be performed in accordance with FAU requirements. If the TOE does not check for multiple authentication failures, then the auditing requirement is reduced to the need to record failed authentication attempts.

Clarification may be required in the Security Target to specify the criteria for time-outs and blocking or re-enabling of authentication attempts against users.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *identifying name or number, unique physical or behavioral characteristic, role, and any other attributes specific to the particular biometric system to be defined by the ST writer*.]

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.

Application Notes:

Typically, authentication is a function provided by a TOE whose main purpose is entirely different (e.g. an office automation network, a numerical analysis system, etc.). In this case, however, authentication is assumed to be the prime purpose of the TOE. It is therefore conceivable that there are no functions provided for the user other than authentication, or the single function of controlling access to a facility or information system, which does not form part of the TOE itself. This security functional requirement (SFR), therefore, expresses the prime objective of the TOE.

Although this SFR applies to authentication of regular users and administrators, the Security Target ***shall*** include FIA_UAU.5 if the TOE provides different or additional authentication mechanisms for administrators. In this case the SFR should identify the different authentication mechanism(s) implemented by the TOE for an administrator and specify the rules governing the use of these mechanisms.

At a minimum, the TOE is required to provide a single-factor biometric authentication mechanism, but is permitted to support multi-factor authentication (e.g., biometric + password/PIN or multiple biometrics). The Security Target ***shall*** include FIA_UAU.5 if the TOE provides multi-factor authentication for users or administrators. In this case, the SFR should identify the multiple authentication mechanisms implemented/allowed by the TOE and specify the rules governing the use and enabling of these multiple mechanisms.

If FIA_UAU.5 is included in a Security Target, this TSF should be identified as an auditable event and the following actions considered for the management functions in FMT:

- management of the authentication mechanism
- management of the rules for authentication

FIA_UAU.3.1

The TSF shall *detect and prevent* use of **biometric** authentication data that has been forged by any user of the TSF.

Application Notes:

In this context, forgery generally refers to the use of an artifact such that the biometric system is spoofed into accepting the artifact as coming from a live human being. It is not possible to make definitive statements on the potential for forging of biometric characteristics. Most biometric characteristics could, in principle, be forged given sufficient resources and justification. The ease will depend on the nature of the biometric, the inherent characteristics of the capture device, and intentional countermeasures implemented in the TOE. For example, in a fingerprint biometric system, there may be some inherent rejection of an inanimate artifact due to the mode of operation of the finger reader (use of total internal reflection and the three dimensional property of a real finger pattern

together with natural skin oil). The developer could also include measurements of temperature, surface conductivity and/or pulse to provide additional countermeasures (i.e., liveness checks) to a fake or disembodied finger. All these would make it harder to produce a viable artifact but would not eliminate the possibility. The developer will need to provide information on inherent and intentional countermeasures to forgery.

The term "biometric authentication data" also includes the biometric template, which may be supplied by the user, e.g. stored on a token. In such cases, the TOE is required to detect and prevent the forged use of a template by an imposter.

This SFR does not explicitly require the ability to detect mimicry by an impostor. Such attacks are not considered as "forgery" of authentication data, rather the TOE meeting the FAR requirements in accordance with O.ADMIN counters these attacks.

The refinement operation has been applied so as to clarify that the requirement concerns forgery of **biometric** authentication data.

FIA_UAU.3.2

The TSF shall *detect and prevent* use of **biometric** authentication data that has been copied from any other user of the TSF.

Application Notes:

This security functional requirement may overlap in some instances with FIA_UAU.3.1 in the case of biometric systems. The production of a forgery may also involve copying the biometric characteristics of an authorized user of a system (i.e. lifting a latent fingerprint from a glass). Most biometric characteristics are not secret and may therefore be vulnerable to being copied. There will be varying degrees of difficulty involved. For example, it may be hard to copy a retinal pattern. This form of copying requires the use of a forgery to exploit the copy.

Replay attacks are not covered by this SFR. FPT_RPL.1 addresses this form of attack.

This SFR does not explicitly require the ability to detect mimicry by an impostor. Such attacks are not considered as "copying" of authentication data, rather, these attacks are countered by the TOE meeting the FAR requirements identified with O.ADMIN.

The refinement operation has been applied so as to clarify that the requirement relates to the copying of **biometric** data.

FIA_UAU.7.1

The TSF shall provide only [assignment: *a text message indicating that verification or identification efforts are underway*] to the user while the **biometric** authentication is in progress.

Application Notes:

This security functional requirement means that the biometric system must not inform the user of any "score" against the threshold that might help the attacker to fool the device in subsequent verification or identification attempts.

The refinement operation has been applied so as to clarify that the requirement relates only to feedback received from the **biometric** authentication mechanism.

FIA_UID.2.1

The TSF shall require each user to identify them self before allowing any other TSF-mediated actions on behalf of the user.

Application Notes:

This security functional requirement is one that needs special interpretation in the context of biometric systems. For this consideration, biometric systems can be considered to divide into two broad categories, identification and authentication. Authentication is where a user makes a claim to be a specific individual and the system authenticates the claimant against the claim. This is analogous to the userid/password authentication in an IT system. Identification is where a user makes no specific claim of identity and the system has to determine who the individual is, or more generally, whether the individual is known to the system. Authentication systems are more common than identification systems but both types are used.

If the TOE is of the authentication type, then the security functional requirement has the same standard interpretation as for an IT password system. A specific claim of identity must be made before the TOE takes any further action. Most commonly, the next action after the user provides identification will be authentication. Note that this SFR applies to both users and administrators. Also, see application note under FIA_UAU.2 above.

If the TOE is of the identification type, then this security functional requirement has no real meaning in the traditional sense. The "identification" action by the user is reduced to presenting the user's biometric to the TOE. The TOE is responsible for the identification and authentication activities in this case.

5.1.2. Security Management Requirements

FMT_MOF.1.1(1)

The TSF shall restrict the ability to *determine the behavior of, disable, enable, or modify the behavior* of the audit mechanism to administrators.

Application Notes:

This is the same requirement as for normal IT system audit logs and trails.

FMT_MOF.1.1(2)

The TSF shall restrict the ability to *enable and disable* the functions: [assignment:
-- perform self-enrollment,
-- perform routine maintenance,
-- perform manual access (e.g., fall-back system),
-- change cryptographic key attributes including key type (e.g., public, private, secret), validity period, and use (e.g., digital signature, key encryption, key agreement, data encryption),
-- rules for authentication (e.g., actions to be taken in the event of user authentication failure, actions allowed before the user is authenticated)
-- revocation rules,
-- emergency start-up/shutdown
-- list of actions that need to be taken in case of repetitive penetration attempts
-- conditions under which TSF self testing occurs, such as during initial startup, --
-- regular interval or under specified conditions
to *administrators.*]

FMT_MOF.1.1(3)

The TSF shall restrict the ability to *enable* the functions [assignment: *to restore the TOE to a secure state from maintenance mode to administrators.*]

Application Notes:

This refers to the functions covered by FPT_RCV.1.1.

FMT_MOF.1.1(4)

The TSF shall restrict the ability to *perform* the *enrollment* functions [assignment: *to administrators or to users permitted for self-enrollment by the administrator.*]

FMT_MTD.1.1(1)

The TSF shall restrict the ability to *modify* the functions [assignment: *ST writer will provide a list of security parameters which control the performance of the biometric system*] to [assignment: *administrators*].

Application Notes:

The security performance of a biometric system is critically dependent on the correct adjustment of threshold values to DoD biometric standards (refer to Appendix A) such as acceptance or rejection of user authentication attempts. This

activity must be restricted to trusted staff (administrators). If this restriction is not properly enforced, the system security will be compromised.

FMT_MTD.1.1(2)

The TSF shall restrict the ability *to initialize, query, modify, delete, or clear* the [assignment: *user security attributes*] the [assignment: *ST writer will supply other system unique attributes such as physical or behavioral characteristics*] to [assignment: *administrators.*]

Application Notes:

Administering the enrolled user database is analogous with administering the user account information in a conventional IT system. In a biometric system, in addition to standard information on users, there will be processes, which enroll users and remove them from the system as required by the system security policy and, possibly, a database of biometric templates for enrolled users. Users must not be allowed to enroll themselves on the system since the system security is totally dependent on the integrity of the enrollment data. These activities must be restricted to authorized administrators and the TOE must impose the restriction.

The partially completed operations are to be completed in the TOE Security Target. The assignment must be completed to list any additional user security attributes included under FIA_ATD.1.1. Then, the selection must be completed as follows: the first item must be selected if biometric templates are stored within the TOE; and the second item must be selected if additional user security attributes have been listed, or if biometric templates are not stored by the TOE.

FMT_MTD.1.1(3)

The TSF shall restrict the ability to *initialize, query, modify, delete, or clear* the [assignment: *audit trail*] to [assignment: *administrators*].

FMT_MTD.3.1

The TSF shall ensure that only secure values are accepted for **enrolled biometric templates**.

Application Notes:

In a biometric system, the level of security achieved is known to be dependent on the quality of the enrolled biometric templates. If a poor enrollment is allowed, then that user may be open to easy attack by an imposter. In this context, a "secure value" for an enrolled biometric template means "an acceptable level of quality".

It is not generally possible for the administrator to make a human judgement of the quality of an enrollment. Therefore, the TOE must be able to assess the quality of the enrollment template and provide a means by which poor

enrollments or null samples can be eliminated. This may be an automatic function of the TOE in rejecting poor quality enrollments and null samples; alternatively, the TOE may provide an indication of enrollment quality to the administrator, allowing the administrator to reject the enrollment. In this case, "secure value" is interpreted to mean "a level of enrollment quality explicitly accepted by an administrator for the individual in question. The role of the administrator in this regard must be clearly stated in the Security Target.

There may be a trade-off between enrollment quality and other factors such as usability. For example, enforcement of a high enrollment quality may exclude certain individuals from enrollment on a system. Therefore, enrollment quality standards should be commensurate with the security requirements for the application. This means that there will generally be a requirement that the TOE allows adjustment by the administrator of the acceptance level standard for user enrollment. The system security policy may specify system-wide standards for enrollment quality but might allow deviations to accommodate individual cases of difficulty. Note, however, that this would introduce a potential vulnerability in the security of the system.

The refinement operation has been performed to clarify the scope of the SFR, replacing the generic term "TSF data" with the specific term "enrolled biometric templates".

FMT_REV.1.1

The TSF shall restrict the ability to revoke security attributes associated with the <u>*users, subjects, objects, and other additional resources*</u> within the TSC to [assignment: *the administrator*].

FMT_REV.1.2

The TSF shall enforce the rules [assignment: *of revoking security attributes upon authenticating the administrator.*]

FMT_SAE 1.1

The TSF shall restrict the capability to specify an expiration time for [assignment: *user templates*] to [assignment: *the administrator*].

FMT_SAE 1.2

For each of these security attributes, the TSF shall be able to [assignment: *deactivate the user template forcing re-enrollment*] after the expiration time for the indicated security attribute has passed.

FMT_SMR.1.1

The TSF shall maintain the roles [assignment: *of users and administrators*].

Application Notes:

Note that it is permissible for a TOE to maintain more than one type of administrator role such as separating the template administration functions from general system administration functions.

5.1.3. Security Audit Requirements

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions.

b) All auditable events for the *basic* level of audit **as defined in Table 5.2**; and

c) [assignment: *other auditable events specific to the particular biometric system as defined by the ST writer*].

Table 5.2 -- Auditable Events

Component	*Auditable Event*	*Additional Information*
Class FIA: Identification and Authentication		
FIA_AFL.1	The reaching of the threshold for the Unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling the terminal)	-
FIA_UAU.2	All use of the authentication mechanism	-
FIA_UAU.3	All immediate measures taken.	Results of checks on the fraudulent data.
FIA_UID.2	All use of the user identification system	User identity provided.
Class FMT: Security Management		
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	-
FMT_MTD.3	All rejected values of *enrolled biometric templates.*	-
FMT_REV.1	All attempts to revoke security attributes	-
FMT_SAE.1	Specification of the expiration time for an attribute	Action taken due to attribute expiration
FMT_SMR.1	Modifications to the group of users that are part of a role.	-
Class FAU: Audit Requirements		
FAU_SAR.1	Reading of information from the audit records.	-
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	-

Component	*Auditable Event*	*Additional Information*
Class FPT: Protection of the Trusted Security Function		
FPT_AMT.1	Execution of the tests of the underlying machine.	Results of the tests
FPT_FLS.1	Failure of the TSF data	-
FPT_ITT.3	The action taken following detection of an integrity error.	-
FPT_RCV.1	The fact that a failure or service discontinuity occurred	Type of failure or service discontinuity.
	Resumption of regular operation	-
FPT_RPL.1	Detected replay attacks.	-
FPT_STM.1	Changes to time.	-
Class FCO: Communication		
FCO_NRO.2	Identification of the information, the destination, and a copy of the evidence provided	
Class FCS: Cryptographic Support		
FCS_CKM.1, .2, .3, .4	The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_COP.1	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	

Application Notes:

A list of any additional auditable events shall be stated in the TOE Security Target by completing the assignment. An assignment of "none" is permissible, in which case paragraph c) should be omitted for the purposes of clarity.

For FMT_MTD.3, the interpretation of the audit requirement is that the audit record must indicate the reason for rejection of a template. Note that successful enrollment is covered by the audit requirement for FMT_MTD.1.

The refinement operation has been applied to include reference to the auditable events listed in Table 2.

FAU_GEN.1.2

The TSF shall record, within each audit record, at least the following information:

a) Date and time of the event, type of event, subject and **individual identity**, and outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *additional information as defined in Table 2 and other audit relevant information specific to the particular biometric system*].

Application Notes:

In some cases, the TOE may not be able to identify the individual identity associated with an event. For example, if the individual is not enrolled in the system, then the TOE can only record the event with an "unknown" identification. Therefore, this requirement should be interpreted as "when the individual is known to the TOE".

Any additional audit relevant information shall be stated in the TOE Security Target by completing the assignment. An assignment of "none" is permissible.

The refinement operation has been applied to replace "subject identity" with the more meaningful term "individual identity".

FAU_SAR.1.1

The TSF shall provide [assignment: *authorized administrators*] with the capability to read [assignment: *audit information*] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.2.3

The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: *audit, storage, exhaustion, failure or attack*.

Application Notes:

The TOE Security Target shall state the metric for saving audit records by completing the assignment. No minimum value is mandated by this PP (except

that "none" is not a valid assignment), providing the metric specified can be justified as sufficient to satisfy the O.RECORD security objective. Audit metrics limit the data loss by inventorying the number of audit records kept and the time that records are guaranteed to be maintained. An example of the metric could be 100,000 indicating that 100,000 records can be stored.

5.1.4. Protection of TSF and Reference Mediation

FPT_AMT.1.1

The TSF shall run a suite of tests *at the request of an administrator* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [assignment: *power failure and physical tampering*].

FPT_ITT.1.1

The TSF shall protect the TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE **and when in storage**.

Application Notes:

The refinement operation has been performed to clarify that TSF data shall always be protected even when stored.

In a biometric system, data flow security includes issues of confidentiality, integrity, and availability. A breach of data flow security could lead to unauthorized individuals being authenticated or authorized users failing to be authenticated. This security functional requirement deals with the confidentiality issues of data flow.

One major transmission of data in a biometrics system takes place between the biometric capture device and the recognition component. A physically open channel in the form of a cable or possibly a remote network connection may separate these components. The possibility of monitoring the data flow between the capture device and the recognition component must be considered as a potential area of vulnerability and the evaluators will be concerned to assess the means by which the TOE protects the data. Protective measures might include physical protection of the data path, detection of attempted monitoring, and data encryption.

A second major data flow comprises the communications of the result of the authentication process to the component which actions the result. An attack mounted on this path could bypass the authentication process altogether. The

TOE Security Target will specify the scope of the TOE and will determine whether and how much of this path is included in the TOE.

Other internal data flows will likely exist and should be considered as potential points of vulnerability. These should be considered in the same way as any IT system handling sensitive data (e.g. for a distributed biometric system, if the enrolled templates are in a remote database, querying that database during user authentication should provide non-disclosed accurate query results).

FPT_ITT.3.1

The TSF shall be able to detect *modification of data* for TSF data transmitted between separate parts of the TOE.

Application Notes:

This security functional requirement deals with the integrity issues of data flow between components of the TOE. The notes addressing confidentiality previously are also applicable to the data integrity issues.

The aspect of data integrity covered here appears to be directed towards compromise caused by deliberate attack. However, other forms of integrity compromise may occur, for example, through hardware malfunction or by external sources of signal interference.

Biometric capture devices are well known to be sensitive to environmental conditions. Typically, stray light or noise (depending on the technology involved) can have a major effect on system performance. This is a data integrity issue though not one which is amenable to analysis in the conventional way. Typically, the TOE will not be able to detect data integrity problems caused by stray illumination or noise and this security functional requirement will need further exploration through functional testing. Stray light or noise can also have an adverse impact on the quality of enrollment.

FPT_ITT.3.2

Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: *prevent access to portal, notify the administrator(s) and audit that event*].

FPT_PHP.3.1(1)

The TSF shall resist [assignment: *physical modification, alteration, replacement or other physical attack*] to the [assignment: *capture device, the comparator function, connection between the capture device and the comparator function, connection between the comparator function and the portal, enrolled template database and connection between the comparator function and the enrolled template* database] by responding automatically such that the TSP is not violated.

FPT_PHP.3.1(2)

The TSF shall resist [assignment: *list of electromagnetic or other relevant noise flooding attacks that may be mounted within the TOE environment*] to the [assignment: *biometric system or its connections*] by responding automatically such that the TSP is not violated.

Application Notes:

It is acceptable for the TOE not to include functionality to resist such physical attacks, provided such attacks are prevented by measures taken within the TOE environment (this is the intention of the qualification that may be mounted within the TOE environment). This must be made clear in the Security Target by listing the relevant attacks that the TOE must resist.

FPT_RCV.1.1

After failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

Application Notes:

If the TOE provided automated recovery procedures for certain types of failures or service discontinuities, then FPT_RCV.2 (or FPT_RCV.3) should be specified in the Security Target. A TOE that meets FPT_RCV.2 or FPT_RCV.3 also satisfies the FPT_RCV.1 requirements and hence is conformant with this PP.

FPT_RPL.1.1

The TSF shall detect replay for the following entities: [assignment: *biometric authentication data and other TSF data exchanged between parts of the TOE*].

Application Notes:

Part of detecting a replay attack is to detect when an "exact match" comparison against a reference template occurs.

FPT_RPL.1.2

The TSF shall [assignment: *ignore the replayed data*] when replay is detected.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Application Notes:

Only one individual at a time can be verified for a single characteristic scan (i.e. two or more individuals cannot gain entry to the portal from a single point). The interval between input for two individuals must be sufficiently small that it is not possible for two individuals to enter on one scan. For example, a face recognition system might be used to verify that the individual using a keyboard remains the same person who was originally verified. The scanning device might be mounted on the monitor and will scan the individual's face periodically. If the scan interval is too large, it would be possible for an illicit individual, in concert with the verified individual, to access the keyboard.

The portal (whether physical or logical), once activated upon successful authentication/identification, must not remain activated illicitly permitting unauthorized individuals access. For a distributed TOE where templates are stored on a server, adequate logical authentication must be provided so that multiple concurrent clients can be supported.

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by un-trusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

FPT_TST.1.1

The TSF shall run a suite of self-tests *at the request of the authorized administrator* to demonstrate the correct operation of the TSF.

FPT_TST1.2

The TSF shall provide authorized *administrators* with the capability to verify the integrity of TSF data.

FPT_TST.1.3

The TSF shall provide authorized *administrators* with the capability to verify the integrity of stored TSF executable code.

Application Notes:

In FPT_TST.1.2 and FPT_TST.1.3 the refinement operation has been applied, replacing "authorized users" with authorized "*administrators"* for the purpose of clarity.

5.1.4.1 Extended FPT Class Security Functional Requirement

FPT_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from* all objects.

Application Note:

This SFR ensures residual biometric data (e.g., biometric samples stored temporarily in the capture device) is not available after its use in the functional component. For example, clearing a biometric sample from the capture device memory after its operation.

5.1.5. Non-Repudiation of Origin Requirements

FCO_NRO.2.1

The TSF shall enforce the generation of evidence of origin for transmitted [assignment: *user templates*] at all times.

Application Notes:

This applies to both externally held user templates on tokens and to enrolled user templates stored locally or remote.

FCO_NRO.2.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

Application Notes:

The TOE Security Target shall complete the assignments by stating the list of attributes of the originator and stating the list of information fields of a user template to which the evidence of origin applies.

FCO_NRO.2.3

The TSF shall provide a capability to verify the evidence of origin of information to *recipient* given [assignment: *limitations on the evidence of origin*].

Application Notes:

The TOE Security Target shall complete the assignment by stating any limitations on the evidence of origin.

5.1.6. Cryptographic Support Requirements

Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *from list of approved cryptographic algorithms in Appendix B*] and specified cryptographic key sizes [assignment: *of:*

- *at least 160 bit private key with at least 1024 bit prime modulus for Digital Signature Standard keys;*
- *at least 1024 bit public key for Key Exchange Algorithm (KEA);*
- *at least 2048 bit public key for RSA;*
- *at least 384 bit for Elliptic Curve Digital Signature Algorithm key prime field (//p//)*]

that meets the following: [assignment: *FIPS 140-2 Level 3 and theX.509 Certificate Policy*].

Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *encryption with key exchange keys for symmetric keys*] that meets the following: [assignment: *FIPS 140-2 Level 3*].

Application note: Possession of the Key Exchange Key authenticates the host to the TOE.

Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1

The TSF shall perform [assignment: *encryption of cryptographic keys in nonvolatile memory*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key storage*] that meets the following: [assignment: *FIPS 140-2 Level 3*].

Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method, [assignment: *zeroization*] that meets the following: [assignment: *FIPS 140-2 Level 3*].

Cryptographic operation (FCS_COP.1)

FCS_COP.1.1

The TSF shall perform [assignment: *signing of hash values and wrapping or unwrapping session keys*] in accordance with a specified cryptographic algorithm [assignment: *from a list of approved cryptographic algorithms in Appendix B*] and cryptographic key sizes [assignment: *of*

- *at least 160 bit private key with at least 1024 bit prime modulus for Digital Signature Standard keys;*
- *at least 1024 bit public key for Key Exchange Algorithm (KEA);*
- *at least 2048 bit public key for RSA;*
- *at least 384 bit for Elliptic Curve Digital Signature Algorithm key prime field (//p//)*]

that meet the following: [*assignment: FIPS 140-2 Level 3 and X.509 Certificate Policy*].

5.2. TOE Security Assurance Requirements

This PP is intended for use with commercial biometric systems, which are deemed certifiable with assurance level EAL4+. In order to claim conformance, developers of biometric products must ensure that the TOE meets or exceeds the EAL4+ assurance components taken from Part 3 of the CC. These assurance components are summarized in the following table.

Table 5.3 -- TOE Assurance Requirements

Assurance Class	Short Title	Assurance Components
Configuration Management	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	Partial CM Automation Generation Support Procedures Problem Tracking CM Coverage
Delivery and Operation	ADO_DEL.2 ADO_IGS.1	Detection of Modification Installation, Generation, and Start-up
Development	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1	Functional Specification High-Level Design Implementation Representation Low-Level Design Representation Correspondence Security Policy Modeling
Guidance Documents	AGD_ADM.1 AGD_USR.1	Administrator Guidance User Guidance
Life Cycle Support	ALC_DVS.1 ALC_FLR.3 ALC_LCD.1 ALC_TAT.1	Development Security Systematic Flaw Remediation Life Cycle Definition Tools and Techniques
Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	Coverage Depth Functional Tests Independent Testing
Vulnerability Assessment	AVA_MSU.2 AVA_SOF.1	Misuse Strength of TOE Security Functions Vulnerability Analysis

	AVA_VLA.2	

5.3. Strength of TOE Security Function Requirements

5.3.1. Minimum SOF Rating

The minimum Strength of Function (SOF) rating provided in this PP is SOF-Medium at EAL4+. In the DoD, this refers to a minimum strength of mechanism level (SML) of 2 as defined in chapter 4 of the *Information Assurance Technical Framework,* which can be found at http://www.iatf.net/. In the event that the TOE provides multiple authentication mechanisms, the minimum SOF rating shall apply to all such mechanisms.

5.3.2. Explicit SOF Metrics

The following requirements only apply to the biometric authentication and identification mechanism(s) implemented by the TOE.

These mechanisms, which implement the FIA_UAU.2 requirement, shall satisfy the DoD biometric standards for False Acceptance Rates (FAR) and False Rejection Rates (FRR) appropriate for EAL4+ as specified in Appendix A.

The SOF analysis will need to be based mainly on a statistical testing approach to confirm that the FAR and FRR requirements are met by the biometric authentication mechanism.

5.4. Security Requirements for the IT Environment

There are no security requirements that must be satisfied by the IT environment.

However, this does not preclude such security requirements being identified in the TOE Security Target, in particular, to satisfy O.USERTMPL in the event that the user provides biometric templates. For example, FDP_DAU.2 together with FCS_COP.1 may need to be defined as requirements on the IT environment to mandate digital signature functionality to sign user templates on enrollment. In such cases, the security assurance requirements shall be at least equal to the security assurance requirements for the TOE.

6. RATIONALE

6.1. Security Objectives Rationale

This section demonstrates that the security objectives identified in Section 4 are traceable to all aspects of the TOE security environment described in Section 3. These objectives are suitable to cover all aspects of the identified environment. Table 6.1 below summarizes the mapping from the security objectives to each of the identified threats, Organization Security Policies (OSPs) and assumptions, in tabular form. This is then followed by a rationale, which justifies the suitability of the security objectives.

	TOE SECURITY OBJECTIVES											ENVIRONMENT SECURITY OBJECTIVES						
	O.ADMIN	O.BYPASS	O.CLEAR	O.CRYPT	O.NO DEGRADE	O.KEY_ ENCRYPT	O.INIT	O.NOFORGE	O.PHYSICAL	O.RECORD	O.USER LIMIT	O.ENROL	O.INSTALL	O.PHYSICAL	O.SECOP	O.TRAIN	O. USER LIMIT	O.USER TMPL
Threats																		
T.ARTIFACT	X							X							X			X
T.BADADMIN																X		
T.BADUSER	X														X	X		
T.BYPASS		X													X	X		
T.CASUAL	X									X	X				X			
T.CORRUPT	X																	
T.CRYPT_ ATTK				X														
T.DEGRADE	X				X								X					
T.EVILTWIN	X											X			X			X
T.FAIL_ SECURE							X											
T.FAKETMPL								X										X
T.FARFRR	X											X			X	X		
T.MIMIC	X											X			X			X
T.NOISE									X						X			
T.POORIMG	X								X			X						
T.POWER	X									X					X			
T.REPLAY				X		X		X										
T.RESIDUAL	X		X					X				X			X			
T.TAMPER									X						X			
T.UNDETECT	X									X					X	X		
T.WEAKID	X											X				X		
Organizational Security Policies																		
P.MANUAL	X														X	X		
P.SECOP															X			
P.TRAIN																X		
P.USERLIMIT	X										X						X	
Assumptions																		
A.NO_EVIL																X		
A.PORTAL																		
A.ROLES	X															X		
A.USERTMPL																	X	

Table 6.1 – Mapping of Security Objectives to Threats, OSPs, and Assumptions

6.1.1. Threats Countered By the Security Objectives

T.ARTIFACT rationale

The threat of the use of an artifact is countered by the following security objectives:

a) O.ADMIN prevents impostors from gaining access to biometric templates stored in the system, and thus reduces the risk that impostors will be able to produce an artifact with an equivalent biometric template.

b) O.NOFORGE reduces the risk of a successful attack based on the use of an artifact, by ensuring that the TOE can detect and prevent the use of forged authentication data, such as an artifact with an equivalent biometric template, to produce an artifact with an equivalent biometric template to that of an authorized user.

c) In a similar way, O.SECOP and O.USERTMPL reduce the risk of an attacker being able to access biometric templates that are not stored on the biometric system, with the intent of producing an artifact with an equivalent biometric template. O.SECOP ensures that impostors cannot access any backups of the enrolled biometric database. O.USERTMPL ensures that there are appropriate measures to control access to biometric templates that are user-held, e.g. stored on a token.

T.BADADMIN rationale

The threat of an administrator unintentionally misusing their authority is countered by O.TRAIN, which provides administrators with appropriate security awareness training. According to A.NO_EVIL, there is no threat of administrators doing so deliberately.

T.BADUSER rationale

The threat of a user attempting to exceed their authority is countered by the following security objectives:

a) O.ADMIN prevents regular users from performing administrative functions such as modifying the parameters of individual users.

b) O.SECOP reduces the risk that an individual user will be incorrectly granted administrative rights.

c) O.TRAIN reduces the risk that users will attempt to exceed their authority by providing individual users with security awareness training.

T.BYPASS rationale

The threat of bypass of the biometric system is countered by O.BYPASS, which prevents such bypassing attacks from being successful.

a) O.BYPASS prevents bypass of the TOE authentication function by an impostor, including by means of either a “hill-climbing” or a “piggy-back” attack.

b) O.SECOP provides for supervision of entry to the portal where necessary; so as to help prevent “hill-climbing” or “piggy-back” attacks.

c) O.TRAIN for administrators reduces the risk of enrollee collusion or security procedure error that might lead to illegal access to the portal either through a “piggy-back” attack, a “hill-climbing” attack, or by substitution following authentication of an authorized user.

T.CASUAL rationale

The threat of a zero-effort attempt is countered by the following security objectives:

a) O.ADMIN ensures by setting an appropriate threshold level (FAR/FRR) that the risk of an imposter making a successful zero-effort attempt is minimized. This limits the chance of a successful attack.

b) O.RECORD provides a deterrent to attackers making a zero-effort attempt by increasing the likelihood that the attacker will be caught.

c) O.SECOP reduces the risk of a successful attack in two ways. Firstly, by ensuring that administrators will regularly check threshold settings which govern the FAR; and secondly, by ensuring that administrators inspect the audit trail on a regular basis, thus increasing the likelihood that the attackers will be caught.

d) O.USERLIMIT limits the ability of imposters to make repeated unchallenged attempts to gain access to the portal. This reduces the chance that a zero-effort attempt will be successful.

T.CORRUPT rationale

The threat of unauthorized modification of security-relevant data is countered by O.ADMIN, which restricts the ability to modify the user security attributes and other security relevant data such as the audit trail and configuration parameters to administrators.

T.CRYPT_ATTK rationale

This threat addresses direct attacks on the cryptographic mechanisms employed in the TOE. This threat is countered by O.CRYPT, which ensures that the available cryptographic functions are of appropriate strength for the sensitivity of the data processed by the TOE.

T.DEGRADE rationale

The threat of degrading the IT environment's existing authentication process by an installed biometric system is countered by the following security objectives:

a) O.ADMIN, which ensures the correct performance of the biometric system.

b) O.NODEGRADE, which ensures that the replacement INA function will be no less secure than the existing INA function.

c) O.INSTALL, which ensures the TOE is delivered and installed correctly to maintain IT security.

T.EVILTWIN rationale

The threat of attack against a similar or twinned ID is countered by the following security objectives:

a) O.ADMIN reduces the risk that the TOE will confuse two individuals by ensuring that the TOE complies with appropriate biometric performance standards (stated in Appendix A). A TOE that meets the O.ADMIN objective will thus limit the number of pairs of individuals that are indistinguishable by the TOE to an acceptable level, and thereby limit the scope for a successful attack by an impostor. O.ADMIN also reduces the risk that an impostor will be able to discover which enrollee(s) they best match by restricting the ability to access the relevant information (e.g. as stored in the enrolled biometric database) to administrators. This will prevent an impostor from being able to perform inter-template comparisons.

b) O.ENROL upholds the quality of the enrolled templates, and hence, supports the TOE in differentiating similar templates.

c) In a similar way, O.SECOP and O.USERTMPL reduce the risk of an attacker discovering which enrollees they best match as a result of being able to access biometric templates that are not stored on the biometric system. O.SECOP ensures that impostors cannot access any backups of the enrolled biometric database. O.USERTMPL ensures that there are appropriate measures to control access to biometric templates that are user-held, e.g. stored on tokens.

T.FAIL_SECURE rationale

O.INIT ensures the TOE always starts in a defined and controlled state regardless of how it was reset. This objective works to prevent attacks that attempt to upset the operation and leave the TOE in an undefined state.

T.FAKETMP rationale

The threat of forgery of a user held template is countered by the following security objectives:

a) O.NOFORGE ensures that the TOE has the capability to detect and thus prevent the use of a forged biometric template.

b) O.USERTMPL ensures that measures exist to provide the means of verifying the authenticity and integrity of user-held templates.

T.FARFRR rationale

The threat of an administrator improperly adjusting FAR/FRR thresholds is countered by O.TRAIN, which provides administrators with appropriate training for setting and maintaining acceptable thresholds. In addition, O.ADMIN and O.SECOP both prevent regular users from performing administrative functions. Since the FAR/FRR thresholds may be adjusted during enrollment, this threat is also countered by O.ENROL, which ensures trained administrators that are capable of adjusting the thresholds appropriately conduct the enrollment process and verify the enrollment is of sufficient quality.

T.MIMIC rationale

The threat of an impostor reproducing biometric characteristics by mimicry is countered by the following security objectives:

a) O.ADMIN addresses the threat that an impostor will be able to successfully reproduce the biometric characteristic of an authorized user through mimicry, by ensuring that the TOE threshold parameters are properly set. A TOE that meets the O.ADMIN objective will thus reduce to an acceptable level, the risk that an impostor will be able to achieve sufficient similarity to the biometric characteristics of an authorized user.

b) O.ADMIN also prevents impostors from gaining access to biometric templates stored on the system, and thus reduces the risk that impostors will be able to practice mimicry of the biometric characteristic.

c) O.ENROL upholds the quality of enrolled templates, and hence supports the TOE in differentiating similar templates.

d) In a similar way, O.SECOP and O.USERTMPL reduce the risk of an attacker gaining access to biometric templates that are not stored on the biometric system, with a view to executing a successful mimicry attack. O.SECOP ensures that impostors cannot access any backups of the enrolled biometric database. O.USERTMPL ensures that there are appropriate measures to control access to biometric templates that are user-held, e.g. stored on a token.

T.NOISE rationale

The threat of flooding with noise data is countered by O.PHYSICAL, which ensures that the TOE is resistant to electromagnetic and other relevant noise flooding attacks, and reflects both TOE and IT environmental considerations. Non-IT environmental considerations are handled by O.SECOP; such that it

requires the individuals responsible for the TOE to perform periodic testing verifying correct operations of the security functions.

T.POORIMG rationale

The threat of an attack directed against a noisy or null biometric sample is countered by the following security objectives:

a) O.ADMIN ensures that the TOE complies with the appropriate biometric performance standards (stated in Appendix A), ensures the TOE verifies the quality of the enrolled templates, and ensures the TOE prevents null biometric samples during enrollment. A TOE that meets the O.ADMIN objective is less likely to have such weaknesses than one that does not meet the objective.

b) O.ENROL upholds the quality of enrolled templates, and thereby reduces the risk of noisy or null biometric sample being accepted during enrollment.

c) O.PHYSICAL ensures that the TOE resists electromagnetic or other relevant noise flooding attacks; thereby, reducing the risk of a noisy biometric input being accepted at the capture device during verification.

T.POWER rationale

The threat of power loss causing a failure in the Biometric System is countered by O.ADMIN, which provides administrators with the capability of restoring the Biometric System to a secure state in the event of failure or interruption. These are supported by O.SECOP, which requires secure operating procedures, which may help prevent power loss, and O.RECORD, which requires an audit trail to isolate specific events such as power failures.

T.REPLAY rationale

The threat of capturing a valid user's biometric authentication data while in transit or storage and later replaying it to gain illicit access or used to attack an higher robustness system is countered by:

a) O.CRYPT, which provides encryption of biometric authentication data including templates while in transit between TOE functional components and while in storage; thus preventing successful capture and replay.

b) O.KEY_ENCRYPT, which provides encryption of any stored keys in non-volatile memory, which further diminishes an adversary's attempt at gaining a decrypted template for the purpose of forgery or replay.

c) O.NOFORGE, which provides the means of performing a live-ness check and detecting forgery of authentication data including detecting exact match comparisons; thus preventing the successful replay of a copied template.

T.RESIDUAL rationale

The threat of illegal enrollment of an impostor is countered by the following security objectives:

a) O.ADMIN reduces the risk that the TOE contains flaws in its design, implementation or operation, that would make it vulnerable to exploitation of residual biometric samples, thus affording illegal entry to the IT or physical portal.

b) O.CLEAR reduces the risk of residual biometric data being present in the TOE after operations are completed.

d) O.ENROL upholds the quality of enrolled templates and hence, supports the TOE in differentiating similar templates.

c) O.NOFORGE reduces the risk of residual biometric samples from being used.

e) O.SECOP reduces the risk of residual biometric templates through requiring procedures governing secure operation of the TOE, which should include regular cleaning of the capture device/sensor.

T.TAMPER rationale

The threat of modification or altering of the software/hardware components or of physical connection between the components or between the biometric system and the portal is countered by O.PHYSICAL, which ensures that the TOE is resistant to such physical attacks and provides for an appropriate level of physical protection within the TOE's IT environment. Non-IT environmental considerations are handled by O.SECOP; such that it requires the individuals responsible for the TOE to perform periodic testing. This verifies the TOE components are intact and the security functions operate correctly.

T.UNDETECT rationale

The threat of undetected attack is countered by O.RECORD, which provides the means to record events, which may indicate attack against the TOE's security functions, and also to provide the capability to hold individual users accountable for their security relevant actions. Auditing addresses after-the-fact attacks; however, knowledge that an attacker might be discovered is often one of the best deterrents. This is supported by:

a) O.ADMIN, which ensures that only administrators have the ability to manage the audit functions and access the audit trail. This reduces the risk of undetected attack arising from a failure to collect sufficient audit data, or from loss of the availability or integrity of audit data. According to A.NO_EVIL, there is no threat of administrators deliberately modifying or deleting audit data so as to cover up their tracks.

b) O.SECOP, which ensures that audit trails are examined on a regular basis. This reduces the risk of undetected impostor attempts and impedes repeated attempts by impostors.

c) O.TRAIN, which will provide administrators with the security awareness training needed in order to be able to identify attempted or actual security breaches from the events recorded in the audit trail.

T.WEAKID rationale

The threat of attack against a weak ID is countered by the following security objectives:

a) O.ADMIN reduces the general risk of weak IDs by ensuring that the TOE complies with appropriate performance standards specified in Appendix A. However, this does not remove entirely the possibility that there will be individuals that have a high FAR. O.ADMIN also reduces the risk that an impostor will be able to discover weak IDs by restricting the ability to access the relevant information (e.g. stored on a token) to administrators.

b) O.ENROL reduces the risk of an insecure enrollment, which might facilitate attack against weak enrollment templates.

c) O.TRAIN for administrators reduces the risk of enrollee collusion that might enable an impostor to discover which are the weak IDs by providing for appropriate security awareness training for administrators.

6.2. OSPs satisfied by security objectives

P.MANUAL rationale

The OSP requirement that a manual means for opening the portal must be provided in the event of a biometric system failure or an emergency situation is satisfied by O.ADMIN, O.SECOP, and O.TRAIN security objectives.

P.SECOP rationale

The OSP requirement that individuals responsible for the TOE execute proper security procedures routinely ensures the IT environment's security is sustained and that the TOE is functioning correctly, which is satisfied by O.SECOP.

P.TRAIN rationale

The OSP requirement that individuals receive appropriate security awareness training is met directly by O.TRAIN.

P.USERLIMIT rationale

The OSP requirement that repeated attempts to gain access to the portal be prevented is met by O.USERLIMIT which is an objective to be satisfied either by the TOE limiting unsuccessful attempts or by environmental measures (e.g. supervised system). O.ADMIN also supports this OSP by providing the administrator with the capability to set the maximum user limit for allowed unsuccessful attempts.

6.2.1. Assumptions are upheld by the security objectives

A.NO_EVIL rationale

This assumption is upheld by O.TRAIN, which is the objective for appropriate security awareness training of individuals.

A.PORTAL rationale

Table 6.1 does not map to any security objectives explicitly to this assumption since it is a general assumption regarding the intended method of use of the biometric system. All security objectives for the TOE and for the environment are based on, and thus can be regarded as, being consistent with or upholding the A.PORTAL assumption.

A.ROLES rationale

This assumption is upheld principally by O.TRAIN, which provides for security awareness training for both administrators and users thus covering their security responsibilities. It is supported by the TOE objective O.ADMIN, which reflect the separation of these roles.

A.USERTMPL rationale

This assumption is upheld by O.USERTMPL, which is the objective for the protection of the authenticity and integrity of user-held templates.

6.3. Security Requirements Rationale

This section demonstrates that the set of security requirements identified in Section 5 are suitable to meet the security objectives identified in Section 4. The following is demonstrated:

a) *That the combination of the individual functional and assurance requirements for the TOE and its IT environment together meet the security objectives.*

   This part of the rationale is provided in section 6.2.1

b) *That the set of security requirements together forms a mutually supportive and internally consistent whole;*

   This part of the rationale is provided in section 6.2.2

c) *That the choice of security assurance requirements is justified;*

   This part of the rationale is provided in section 6.2.3

d) *That the selected strength of function level for the PP, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.*

This part of the rationale is provided in section 6.2.4

6.3.1. Suitability of security requirements

Table 6.2 maps the security functional requirements (SFR) for the TOE and for the IT environment to the security objectives identified in Section 4.

Table 6.2 -- Functional Component to Security Objective Mapping

Security Objectives	Functional Component
O.ADMIN	FIA_ATD.1 FIA_AFL.1 FIA_UID.2 FIA_UAU.2 FMT_MTD.3 FMT_SMR.1 FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MOF.1(4) FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FPT_RCV.1 FPT_AMT.1 FPT_TST.1
O.BYPASS	FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FPT_ITT.1 FPT_ITT.3 FPT_RVM.1 FPT_SEP.1
O.CLEAR	FPT_RIP.2 (extended FPT requirement)
O.CRYPT	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
O.INIT	FPT_RCV.1 FIA_UID.2
O.KEY_ENCRYPT	FCS_CKM.3
O.NODEGRADE	FPT_SEP.1
O.NOFORGE	FCO_NRO.2 FIA_UAU.3 FPT_ITT.1 FPT_ITT.3

Security Objectives	Functional Component
	FPT_RPL.1
O.PHYSICAL	FPT_PHP.3(1) FPT_PHP.3(2)
O.RECORD	FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FAU_STG.2 FMT_MOF.1(1) FMT_MTD.1(3) FPT_STM.1
O.USERLIMIT	FIA_AFL.1

The following rationale shows, for each TOE security objective in turn, why the security requirements are suitable. This discussion focuses naturally on the role of the SFRs, although the role of specific security requirements is also discussed where they have direct relevance to a security objective.

O.ADMIN rational

The objective to provide administrative functions that are limited to administrators is met by the following SFRs:

a) FIA_AFL.1 allows the administrator to set the maximum user limit of unsuccessful verification attempts.

b) FIA_ATD.1 assists the administrator in maintaining the list of security attributes belonging to individual users.

c) FIA_UID.2 and FIA_UAU.2 provide support to the achievement of this objective by requiring identification and authentication of administrators.

d) FMT_SMR.1 requires the TOE to be able to recognize the administrator role, and to be able to associate users with that role.

e) FMT_MTD.1(1) requires that the ability to tune the performance of the biometric system be restricted to administrators.

f) FMT_MTD.1(2) requires that the ability to maintain the user security attributes be restricted to administrators.

g) FMT_MOF.1(1) and FMT_MTD.1(3) require that the ability to manage the auditing functions be restricted to administrators. Table 6.2 maps the security functional requirements (SFR) for the TOE and for the IT environment to the security objectives identified in Section 4.

h) FMT_MOF.1(2), FMT_MOF.1(3), and FMT_MOF.1(4) require that the ability to allow: self-enrollment, routine maintenance performance, manual access for fall-back, emergency start-up/shutdown all be restricted to administrators. FMT_MOF.1(4) further provides a layer of oversight by permitting a user to self-enroll only if authorized by the administrator.

i) FPT_RCV.1 requires the provision of the capability to restore the TOE to a secure state in the event of a failure or service interruption, entering the TOE into a maintenance mode where the capability to return the TOE to a secure state is provided. FMT_MOF.1(3) requires that the capability to perform such restoration from maintenance mode is restricted to administrators.

j) FPT_TST.1 and FPT_AMT.1 require the TOE to provide administrators with the capability to periodically validate the correct operation of the TSF and its underlying abstract machine, respectively.

k) FMT_MTD.3 requires the TOE to ensure only secure values are accepted for biometric templates; thus, ensuring good quality templates during enrollment.

O.BYPASS rationale

The objective to prevent bypass of TOE security policy enforcement is met by the following SFRs:

a) FIA_ATD.1 ensures the TSF is maintaining the list of security attributes thereby preventing bypass of the biometric system.

b) FPT_RVM.1 prevents bypass of the TSP enforcement functions by requiring that they are invoked and succeed before each function within the TOEs scope of control is allowed to proceed. FPT_SEP.1 further prevents bypass by requiring the TSF to maintain a security domain for its own execution; thus, protecting it from interference and tampering by un-trusted subjects.

c) FIA_UID.2 and FIA_UAU.2 require users to be successfully identified and their claimed identity authenticated prior to entry through the portal, in particular, preventing access to any functionality prior to user identification and authentication that might be exploited to bypass TSP enforcement.

d) FIA_UAU.7 prevents bypassing attacks by limiting feedback information displayed to the user during the verification process. By providing limited feedback (e.g., only a text message indicating “in progress”), adversaries are not given sufficient scoring information needed to bypass the biometric system.

e) FPT_ITT.1 prevents bypassing attacks based on attempting to intercept confidential TSF data when it is transmitted between separate parts of the

TOE, e.g. between the biometric capture device and the recognition component.

f) FPT_ITT.3 prevents bypassing attacks based on attempts to compromise the integrity of TSF data when it is transmitted between separate parts of the TOE.

O.CLEAR rationale

The objective to prevent unauthorized access by using residual biometric data is met by an extended security functional requirement FPT_RIP.2 that ensures any previous information content of a resource is made unavailable after its use.

O.CRYPT rationale

Enrolled templates and biometric data are prevented from being disclosed and modified by O.CRYPT. O.CRYPT is implemented by FCS_COP.1 (cryptographic operation) that specifies how the TOE will perform specific cryptographic operations. FCS_CKM.1 (cryptographic key generation), FCS_CKM.2 (cryptographic key distribution), and FCS_CKM.4 (cryptographic key destruction) require that cryptographic keys be generated, distributed, and destroyed in accordance with specified methods of sufficient strength.

O.INIT rationale

FPT_RCV.1 and FIA_UID.2 ensure the TOE always starts in a defined and controlled state regardless of how it was reset and user authentication is always invoked.

O.KEY_ENCRYPT rationale

To protect keys stored within the TOE's non-volatile memory from disclosure, O.KEY_ENCRYPT requires encryption of stored keys. This is satisfied through FCS_CKM.3, which ensures that access to cryptographic keys is in accordance with a specified access method and based on an assigned standard.

O.NODEGRADE rationale

The objective to prevent degrading the security of the IT environment's authentication process is met by FPT_SEP.1, which provides separation between subjects within the TSC.

O.NOFORGE rationale

The objective to detect and prevent forgery of authentication data is met by the following SFRs:

a) FIA_UAU.3 states that the Biometric System must distinguish between forgeries of any kind particularly live from non-live input. FIA_UAU.3.2 requires that one individual cannot use the enrolled biometric data for another user. For example, the biometric system should be able to detect an attempted use of a voice recording.

b) FCO_NRO.2 enforces the generation of evidence of origin for transmitted templates at all times. This applies to templates that are externally provided on a token, stored locally to the comparison function and stored remotely to the comparison function. This SFR provides non-repudiation proof of origin and ensures the template is not forged.

c) FPT_ITT.1 prevents attempts to intercept confidential TSF data when it is transmitted between separate parts of the TOE, e.g. between the biometric capture device and the recognition component. Such attempts may be made with the intent of copying authentication data, and using this data to perform a forgery attack.

d) FPT_ITT.3 requires the TOE to detect attempts to compromise the integrity of TSF data when it is transmitted between separate parts of the TOE, thereby helping to prevent attempted forgery attacks.

e) FPT_RPL.1 requires the TOE to block attacks based on the capture and replay of biometric authentication data.

O.PHYSICAL rationale

The objective to prevent physical attacks on the TOE is met by the following SFRs:

a) FPT_PHP.3(1) requires the TOE to resist physical attacks such as physical alteration, modification, or replacement of its components or of the connections between those components.

b) FPT_PHP.3(2) requires the TOE to resist electromagnetic or other relevant noise flooding attacks where these are not precluded by the TOE environment.

O.RECORD rationale

The objective to provide the means of detecting and recording security relevant events is met by the following SFRs:

a) FAU_GEN.1 requires the capability to generate records of security relevant events, including the identity of the user responsible in order to be able to hold users accountable for their actions.

b) FAU_SAR.1 requires the TOE to provide administrators with the ability of reviewing the audit data so as to be able to identify security relevant events and assess their impact. FAU_SAR.2 requires that the ability to read the audit records be restricted to the administrator.

c) FAU_STG.2 requires the TOE to minimize potential loss of audit data in the event of audit storage exhaustion, failure or attack, and to prevent compromise

of the integrity of the collected data through unauthorized modification or deletion.

d) FMT_MOF.1(1) and FMT_MTD.1(3) requires the TOE to provide the administrators with the ability to manage the auditing functions.

e) FPT_STM.1 requires the provision of reliable timestamps that the ability to manage the auditing functions and the audit trail be restricted to administrators. These SFRs thus help to ensure that the appropriate audit data is collected and maintained by the TOE.

O.USERLIMIT rationale

The objective to limit user authentication attempts is met by FIA_AFL.1. Note however, that it is permissible for the TOE not to provide such functionality, providing this is clearly stated in the ST. In such cases, the objective is to be satisfied by the environment, as stated in Section 4.

6.3.2. Mutually supportive requirements

Table 5.1 lists the dependencies of each CC Part 2 functional component included in this PP. It can be readily seen by inspection that all dependencies on other functional components are satisfied within the set of SFRs mandated by the BPP (Medium). All dependencies between assurance components are satisfied for assurance level EAL4+, as defined in CC Part 3, to be a self-contained assurance package.

In addition to the dependencies between functional and assurance components, there are additional instances of support between SFRs in particular that exist to ensure that the set of requirements form a mutually supportive and cohesive whole.

The primary function of the biometric system, namely identification and verification of users, is provided by SFRs from the FIA class. The SFRs selected from the FAU class provide auditing functions in support of the FIA requirements by detecting security relevant events that might indicate a potential compromise of those functions. These are, in turn, supported by SFRs from the FMT and FPT classes as follows:

a) SFRs from the FMT class provide administrator functions to support secure management of the security functions and of TSF data such as the user security attributes and the audit trail (on which the FIA and FAU SFRs depend).

b) SFRs from the FPT class provide appropriate protection of the TSF, preventing bypass of the security functions (FPT_RVM.1), protecting TSF data (FPT_ITT.1, FPT_ITT.3, FPT_TST.1), blocking replay attacks (FPT_RPL.1), resisting physical attacks against the Biometric System (FPT_PHP.3), validating correct operation of the TSF (FPT_AMT.1, FPT_TST.1), and providing a self protecting TSF (FPT_SEP.1).

Finally, the security assurance requirements are by definition supportive of the SFRs. Section 6.2.1 above cites specific cases where individual assurance requirements help to achieve the security objectives and thus support the relevant SFRs in so doing.

6.3.3. Assurance security requirements rationale

Assurance is that property of the Biometric System, which gives confidence that the security functions are effective and are implemented correctly. This comes from an understanding of how the Biometric System is defined, constructed, maintained, and operated.

The first factor considered in the selection of the EAL4+ assurance level was the value of the assets to be protected by the Biometric System and the risk associated with their compromise. The higher the value of assets to be protected and the greater the risk to those assets, the higher the assurance level that is needed.

A second consideration in the selection of the assurance level was the current state of practice in the definition and construction of commercially available biometric technologies. Higher assurance levels have more stringent requirements and at some point, the assurance level requirements exceed the current state of practice. However, it was determined that an assurance level of EAL4+ would be within the reach of commercially available Biometric Systems. Higher assurance levels will be addressed in the DoD Biometric System Protection Profile (High) and will have to be designed and implemented with the specific assurance requirements in mind. EAL4+, therefore, represents an appropriate level of assurance for this PP.

The third factor considered in the selection of the assurance level was the cost and schedule. Development costs, evaluation costs, and maintenance costs coupled with the impact on "time to market" projections for commercial vendors were held in perspective during the development of this PP. If the stated assurance level is unrealistically demanding, then the associated costs may very well outweigh the benefits and, consequently, be prohibitively high for the biometric industry. Consequently, this document represents one of three in a family of PPs for the Department of Defense (BPP Basic, BPP Medium, and BPP High) and allows vendors to cite conformance without having to meet the demanding functional and assurance requirements of our most discreet high assurance users.

6.3.4. Strength of TOE Security Functions Rationale

The minimum SOF rating (Basic, Medium, High) and the explicit strength metrics (FAR, FRR) are determined by the Department of Defense (DoD). The minimum SOF for TOEs compliant with this PP is SOF-medium. Since T.FARFRR is directly satisfied by the security objective O.ADMIN, it follows that the SOF requirements are consistent with the security objectives of the TOE.

The minimum SOF does not apply to any cryptographic mechanisms with respect to a CC evaluation. The strength of cryptographic algorithms is outside the scope of the CC. The strength of the cryptographic mechanisms will be determined by NIST FIPS 140-2 certification, the tests included in this PP, and any covert channel analysis conducted on the cryptographic module.

6.4. Dependency Rationale

Table 5.1 lists all security functional requirements and the applicable dependent requirements (SFR). The dependent security requirement, FMT_MSA.2 (for the SFRs: FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, and FCS_COP.1), is not required to be met in this PP, if cryptographic keys are generated in accordance with FCS_CKM.1.1 and encryption is performed in accordance with FCS_COP.1.1 (i.e., using the approved list of cryptographic algorithms in Appendix B and using the specified key sizes).

References

1. *Common Criteria for Information Technology Security Evaluation,* CCIB-98-031, Version 2.1, August 1999.

2. *U.S. Government Traffic Filter Protection Profile for Medium Robustness Environments,* Version 1.4, May 2000.

3. *Biometric Device Protection Profile*, DRAFT, Version 0.82, U.K. Government Biometrics Working Group, September 2001.

4. *Department of Defense Directive, Information Assurance (IA), Number 8500.aa,* DRAFT, dated 15 November 2001, and *Department of Defense Instruction, Information Assurance (IA) Implementation, Number 8500.bb,* DRAFT, dated 26 November 2001.

5. *Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness*, Version 1.22, May 2001.

6. *Department of Defense Public Key Infrastructure (PKI) Token Protection Profile*, Version 2.0, March 2001.

7. *National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standard Publication (FIPS-PUB) 140-2,* dated May 25, 2001.

8. *X.509 Certificate Policy for the United States Department of Defense*, version 5.2, dated 13 November 2000.

9. Biometrics Application Programming Interface (BioAPI) specifications, available at www.bioapi.org

Acronyms

Acronym	Definition
CC	Common Criteria
BMO	Biometrics Management Office
EAL	Evaluation Assurance Level
FAR	False Acceptance Rate
FIPS	Federal Information Processing Publications
FRR	False Rejection Rate
INA	Identification and Authentication
NFA	Number of false acceptances
NIIA	Number of imposter identification attempt
NIIV	Number of imposter verification attempts
OSP	Organizational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
PKI	Public Key Infrastructure
SBU	Sensitive But Unclassified
SFR	Security Functional Requirements
ST	Security Target
SOF	Strength of Function
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

D R A F T

APPENDIX A

U.S. Biometric Performance Standards

Table A, defined by the Department of Defense (DoD) Biometrics Management Office (BMO), specifies version 1.0 of the U.S. accuracy performance measures for biometric systems implemented for DoD environments requiring medium robustness.

Table A – Biometric Performance Standards for Medium Robustness Environments

Information Security Robustness Level	Accurate Rejection Rate (1-FAR)
MEDIUM	ARR ≥ 0.9999

Legend:
FAR – False Acceptance Rate – the percentage of imposters wrongly matched

Formula: FAR = NFA/NIVA
FAR: False acceptance rate
NFA: The number of false acceptances
NIVA: The number of imposter and incorrect verification attempts

APPENDIX B

Approved Cryptographic Algorithms

The following cryptographic algorithms are approved for use with biometric systems:

Signature Algorithms:
1024 bit RSA
2048 bit RSA
DSA 1024 (SHA-1)
Elliptic Curve Digital Signature Algorithm 384

Key Exchange Algorithms:
1024 bit RSA
2048 bit RSA
Diffie-Hellman 1024
KEA 1024
Elliptic Curve Key Exchange Algorithm 384

Symmetric Algorithms:
AES (128, 192 and 256 bit keys)
DES 64
Triple DES 128
Skipjack

Hash Algorithms
SHA-1
MD-5
SHA 256
SHA 384
SHA 512

Any other NIST-approved cryptographic algorithms.